The National Committee on Vital and Health Statistics

The Public Advisory Body to the Secretary of Health and Human Services

SUB-COMMITTEE ON STANDARDS

Health IT Advances in Privacy and Security

June 11, 2014

New Concepts in Health Information Privacy and Security

- Data Segmentation for Privacy and Provenance
- Metadata Tagging/Labeling for Security and Privacy
- National standards for coding confidentiality, sensitivity and integrity
- eConsent
- Data Provenance
- NSTIC – the National Strategy for Trusted Identity in Cyberspace

Basic Drivers for New Approaches to Health Information Privacy and Security

- Sensitivity around privacy of information continues to grow
  - Ongoing exposures and breaches of data
- Higher expectations for patient engagement in care
  - "Nothing about me without me"
- Rapid adoption of EHRs
  - Larger amounts of information available electronically
  - New requirements and expectations (i.e., Meaningful Use)
- Expanded demands for exchange of health information
  - Health Information Exchanges
- HIPAA Privacy and Security and State Privacy Regulations
  - HIPAA Omnibus Rule; Accounting of Disclosures; New state mandates
- Increased expectations of patient controls over their information
  - What to access, by whom, for what purpose, when, how…

Key Definitions

- eConsent:
  - The electronic mechanism to allow consumers to express privacy preferences regarding the collection, maintenance, transfer, access, use or disclosure of their health information

- Data Segmentation:
  - Process of sequestering from capture, access, view or disclosures certain data elements that are perceived by a legal entity, institution, organization or individual as being undesirable to share

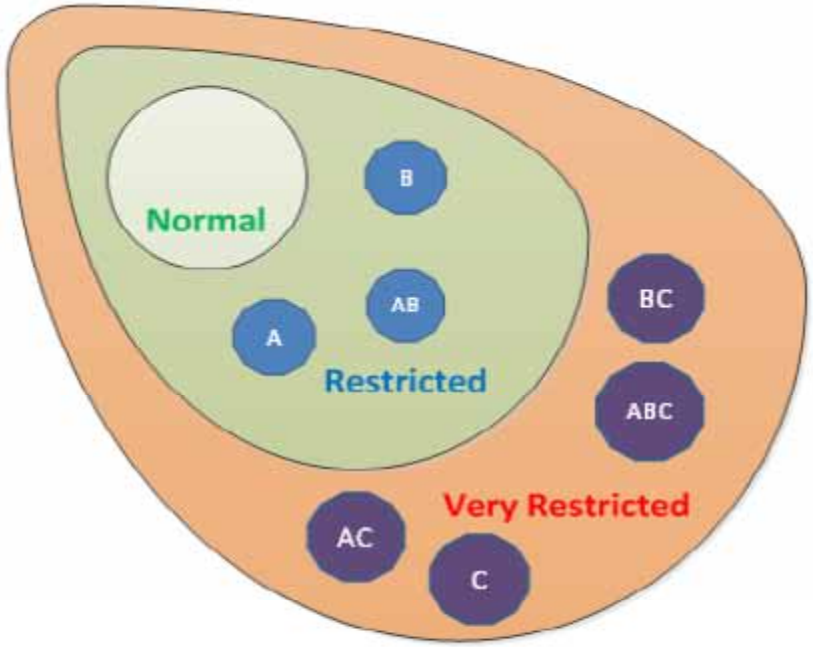
Key Definitions

- Metadata/tag:
  - A tag is a keyword or term assigned to a piece of information (data about data) that helps describe a condition or characteristic of the information for purposes of further action
- Security Labeling:
  - Process for attaching metadata tags to convey information used by systems to determine how to handle data communicated between those systems.
  - Security labels are used to control access, specify protective measures, determine additional handling restrictions of data
- Provenance:
  - Attributes about the origin of health information at the time it is first created, and that tracks the uses and permutations of the health information over its lifecycle.

Segmenting with Security Labels

- **Security Labels are placed on to documents and other information for two reasons: (ISODE Security Label)**

1. **To clearly label information in an unambiguous manner, in order to facilitate human and computer handling of the information,**

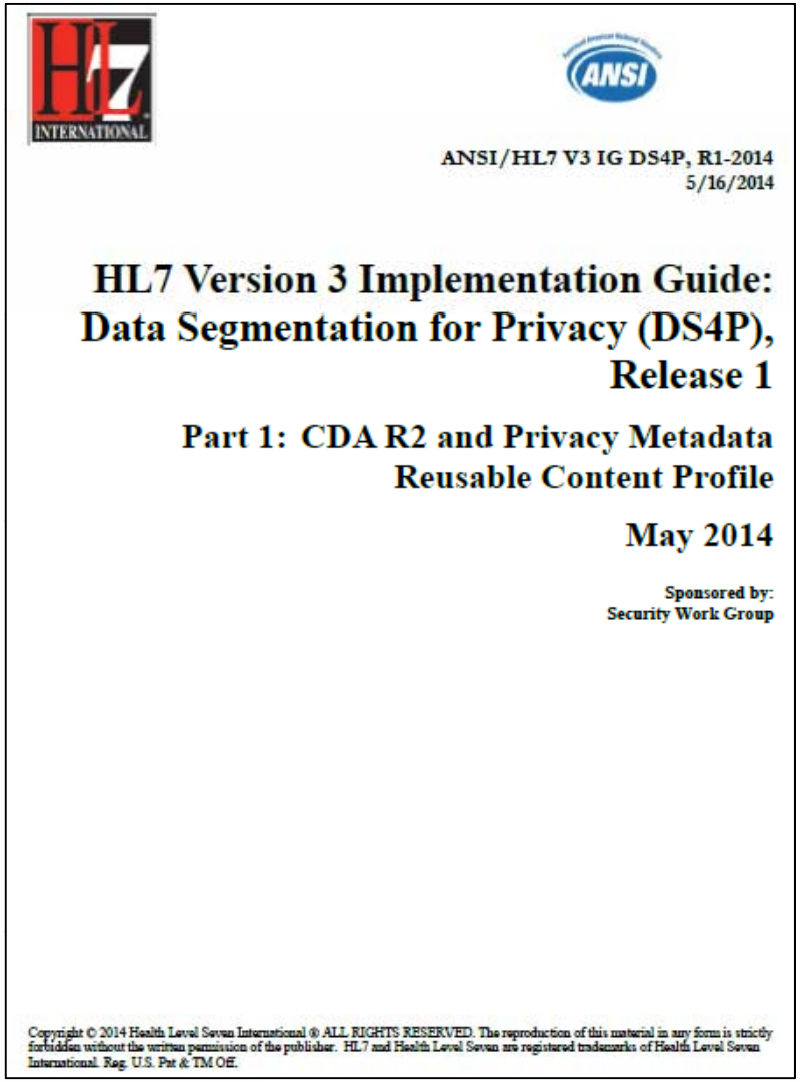


2. To enable a computer to perform Access Control operations on the information, so that the information is accessed only by appropriately cleared people in appropriate locations.

Levels:
-- Document
-- Section/Segment within document
-- Data element within section/segment

Data Segmentation for Privacy

- Standard that allows electronic clinical documents in CDA form to be tagged (at the document or segment level) with information that allow systems to
  - Exclude the data from being accessed/used/disclosed
  - Transmit the 'tags' or metadata to others to inform them about privacy and security conditions and characteristics of the data
- Passed and approved as a NORMATIVE standard
- Ready for adoption and implementation



ANSI/HL7 V3 IG DS4P, R1-2014
5/16/2014

HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1

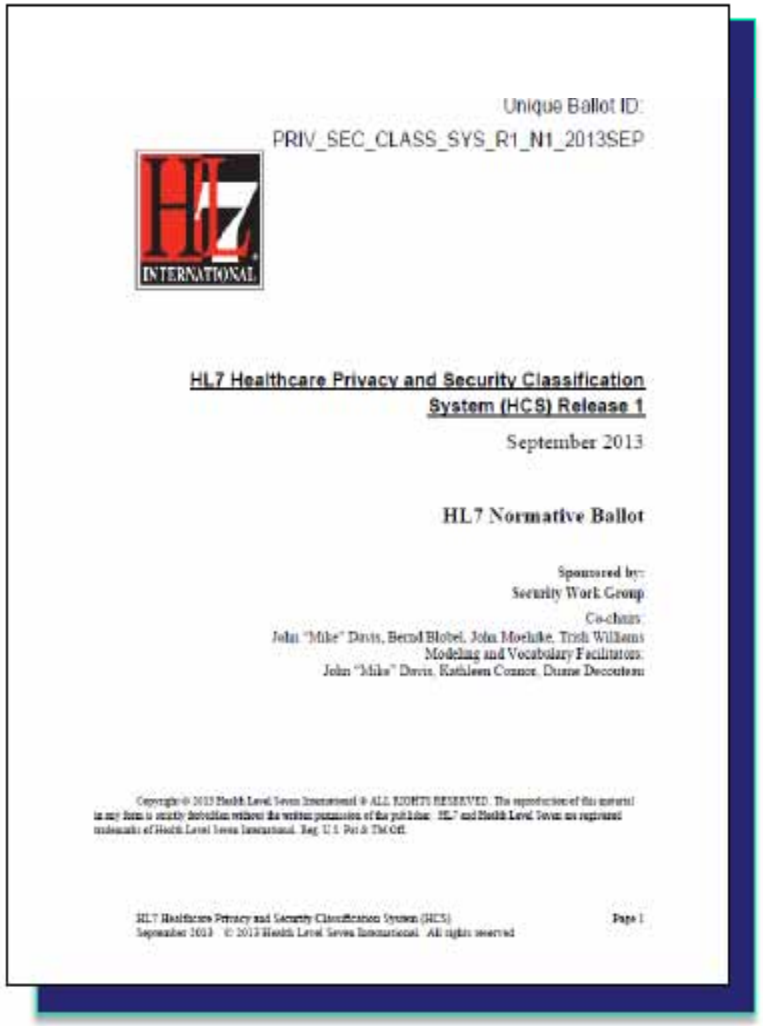
Part 1: CDA R2 and Privacy Metadata Reusable Content Profile

May 2014

Sponsored by:
Security Work Group

International Standards for Health Care Privacy and Security Classification

- Health Level 7 (HL7) Healthcare Privacy and Security Classification System
- Utilizes “Russian doll” nested concept of applying metadata tags
  - Document level
    - Segment level
      - Element level
- Security labels bind clinical data to patient consent
- Security labels use standard classification codes that include:
  - Confidentiality, Sensitivity, Provenance, Integrity, Compartment
  - Purpose, Obligations, Refrain Policy



Unique Ballot ID:
PRIV_SEC_CLASS_SYS_R1_N1_2013SEP

HL7 INTERNATIONAL

HL7 Healthcare Privacy and Security Classification System (HCS) Release 1

September 2013

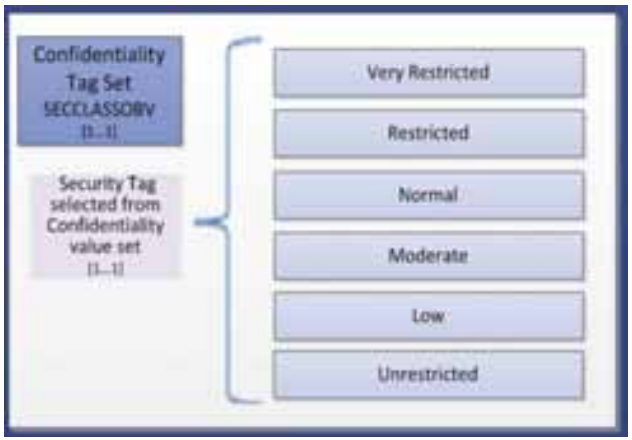
HL7 Normative Ballot

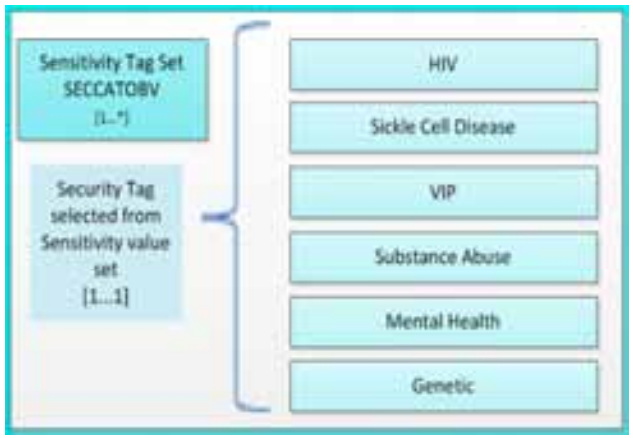
Sponsored by:
Security Work Group

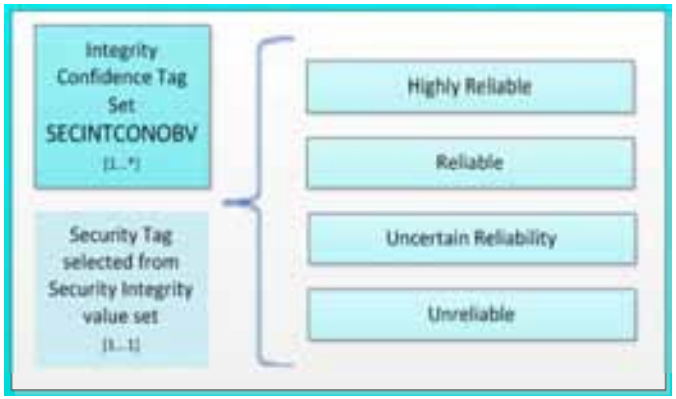
Co-chairs:
John "Mike" Davis, Bernd Blobel, John Moehike, Trish Williams

Modeling and Vocabulary Facilitators:
John "Mike" Davis, Kathleen Connor, Duane Decouteau

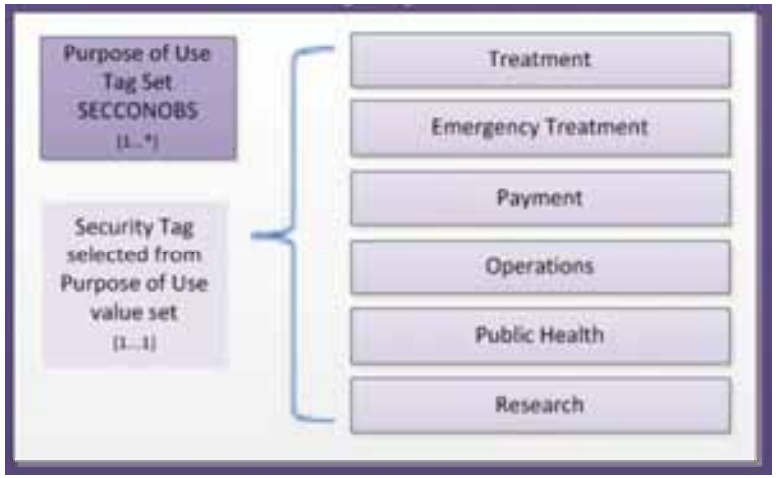
Standard Health Information Privacy and Security Coding System

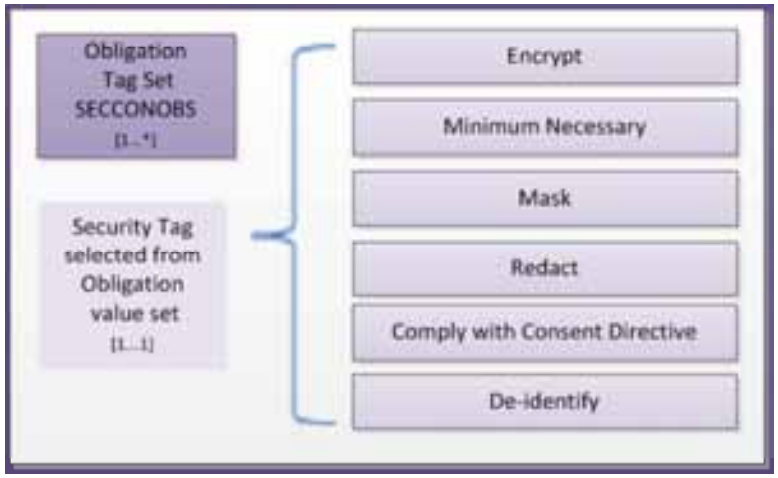


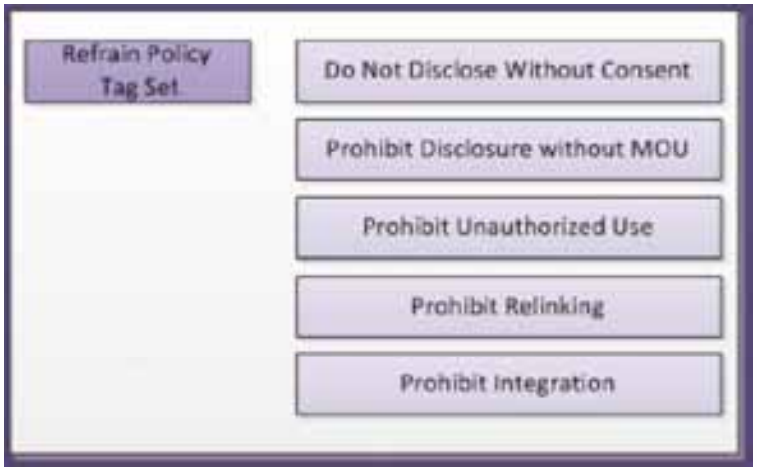




Standard Health Information Privacy and Security Coding System







Data Provenance

- Highlighted as a priority area for action in the 2011 PCAST Report
- Uses similar metadata/tagging concepts as data segmentation
  - Various levels (Document, Section/Segment, Data Element)
  - Various factors (author, entity, system source, date/time stamp)
  - Need to convey with confidence the authenticity, reliability and trustworthiness of health information being exchanged
  - Need to have a clear trail of provenance to validate and decide to rely upon and use the data

Data Provenance

- Current efforts:
  - S&I Framework initiated a “Data Provenance” initiative 2 months ago
    - Issue: no existing authoritative spec, standard or model for provenance for health information
    - Initiative Goal:
      - Establish guidance for handling data provenance in content standards, including the level to which provenance should be applied
      - Establish the minimum set of provenance data elements and vocabulary
      - Standardize the provenance capabilities to enable interoperability

Status of Development

- Phases
  - Phase 1 – Consensus on Charter and Scope (completed)
  - Phase 2 – Identification and definition of Use Cases (underway)
  - Phase 3 – Use Cases Harmonization and Standards Identification and Evaluation
  - Phase 4 – Pilots
  - Phase 5 – Evaluation
- Outcomes
  - Implementation guidelines, models
  - Standards artifact(s) to be vetted via Standards Organizations

The National Strategy for Trusted Identity in Cyberspace (NSTIC)

- 2013 President's Initiative that calls for "… a strategy to make online transactions more secure for businesses and consumers alike… to foster growth and innovation online and across our economy"
- What is it? A new Identity Ecosystem in which individuals and organization performing online transactions are uniquely, unambiguously and securely identified through the use of identity keys and certificates
- How it applies to health care? Ecosystem will support the identification of individuals (consumers, patients, providers) and organizations conducting transactions
- Where is it today? Currently being piloted in various industries, including health care; expecting role-out by 2016

Putting It All Together

- Participants in a transaction (for example, an information exchange) including patients, providers are uniquely identified through NSTIC
- Organization defines its privacy and security policies (based on external policy requirements, internal organization policies)
- Consumer set preferences via eConsent
- Security Tags are dynamically attached to patient information
  - Defining levels of confidentiality, sensitivity, integrity, provenance, purpose of use
  - Purpose of Use, Obligations, Refrain Policy
- Access, use or disclosure of health information is performed based on Security Tags
- Tags are attached to data that is disclosed, so that recipient can incorporate, validate, and execute

Current Realities and Future Expectations

- Most of these concepts are currently being developed in the U.S.
- The national/international standards have been created and are being tested and validated
- At least one organization has began to implement security tagging and segmentation (Veterans Administration)
- No federal or state policy currently exists that requires all these elements
  - One federal program requires segmentation (42 CFR Part 2 for Substance Abuse information)
- It is expected that Phase III of Meaningful Use (to start in 2017) will incorporate several of these concepts as required capabilities of Certified EHRs