



Health IT Standards Committee
Meeting Summary
October 21, 2011

[Meeting Agenda](#)

Background

The [Health IT Standards Committee](#) is charged with making recommendations to the National Coordinator for Health IT on standards, implementation specifications, and certification criteria for the electronic exchange and use of health information. In developing, harmonizing, or recognizing standards and implementation specifications, the Health IT Standards Committee will also provide for the testing of the same by the National Institute for Standards and Technology (NIST).

Opening Remarks (John Halamka)

- ◆ Today's meeting is to polish the committees work and receive additional recommendations

HITSC Privacy and Security Workgroup (Dixie Baker, Chair)

- ◆ General Recommendations (most important recommendation of the day)
 - Effective integration of EHR, infrastructure, and specialized security products and services is key to protecting electronic health information, care quality, and patient safety
 - Today every Complete EHR and EHR Module must meet all security certification criteria – which tends to encourage the implementation of security services within the EHR, rather than having the EHR use stronger mechanisms provided by the infrastructure or third-party services
 - To enable the certification process to more effectively address security integration, we recommend that the ONC and NIST consider modifying the certification process so that each privacy and security certification criterion is treated as “addressable” – to meet the criterion, each Complete EHR or EHR Module submitted for certification would need to either:
 - a) Implement the required security functionality within the Complete EHR or EHR Module(s) submitted for certification; or
 - b) Assign the function to a third-party security component or service, and demonstrate how the certified EHR product, integrated with its third-party components and services, meets the criterion
- ◆ Consumer Communication Recommendations - All **NEW** in Stage 2
 - Use at least one factor (e.g., password) to authenticate the identity of consumer or personal representative
 - Exchange messages securely
 - Authenticate consumer
 - Authenticate EHR
 - Encrypt and integrity protect message
 - Standards: FIPS Pub 140-2, transport layer security (TLS), secure email (SMTP/SMIME)
 - Implementation Specifications: NIST SP 800-52 (TLS); NwHIN transport specifications
 - Security download of health information
 - Include data provenance with downloaded information and information sent to PHR
 - Warning before PHI download should be “guidance” or “best practice” and not certification criterion
- ◆ General Privacy and Security
 - No changes recommended for the following criteria
 - a) Access Control
 - b) Accounting of Disclosures

- c) General Encryption
 - d) Accounting of Disclosures
- ◆ General Privacy and Security Recommended Changes
 - Automatic Log-off: Clarify “terminate a session” criterion to include:
 - a) Session lock after designated period of inactivity
 - b) Session unlocking with user authentication
 - c) Session termination (automatic log-off) after designated period of inactivity
 - d) Capability to designate time periods for session locking and termination
 - Audit Log:
 - a) Change title to “Activity Auditing” (as recommended by IWG)
 - b) Broaden scope, and allow more selectivity, for security auditing
 - Require detection of, and recording of information about “security-relevant events” – rather than “actions related to electronic health information” only
 - Change standard to “Record audit data about security-relevant events” – replacing limited enumerated list of data elements and events
 - Add ASTM E2147-01 as implementation specification (suggests data elements and events)
 - c) Add audit-data protection provisions
 - Integrity: Add SHA-2 as a standard (but retain SHA-1)
 - Authentication: Separate criteria for person vs. entity
 - a) Person authentication – at least single factor (e.g., password)
 - b) Entity authentication – X.509 digital certificates
 - Encryption: Incorporate provisions of “Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals,” issued by the Secretary per ARRA/HITECH breach-notification provisions
 - a) Add criterion for encryption for data-at-rest on end-user devices:
 - “Data-at-rest encryption. EHR technology whose functionality includes the capability to manage electronic PHI on end-user device storage must be able to encrypt and decrypt data persisted on those end-user devices.”
 - b) Encryption when exchanging electronic health information:
 - Add standards: transport layer security (TLS), Internet Protocol security (IPsec)
 - Add implementation specifications cited in breach guidance, plus NWHIN transport standards
- ◆ General Privacy and Security NEW Objectives/Measures
 - Encryption of data at rest in data centers and mobile devices
 - a) Recommended encryption for data on end-user devices controlled by EHR
 - b) Encryption of data in data centers is risk-management decision – and out of scope for certification criteria (as suggested by IWG)
 - Two-factor authentication: agree with IWG assessment as out of scope
 - Entity-level digital certificates: Incorporated into entity authentication criterion
 - Detect and block programmatic attacks (e.g., lock-out after allowed number of log-in attempts): does not align well with today’s identity authentication technologies; suggested that HITPC consider “guidance” or “best practice” rather than policy
 - Amendments to health records:
 - a) Amendment by authorized provider, while preserving data integrity
 - b) Attachment of patient assertion and provider rebuttal

- c) Audit trail of amendments
- d) Recommend the Implementation Workgroup have an expert in medical records review the criteria we have suggested
- ◆ General Recommendation on Stage 2 MU to Implementation Workgroup
 - While discussing potential privacy and security criteria for Stage 2, we often found ourselves discussing whether “the EHR” (Complete or Module) submitted for certification should be expected to meet a given criterion, or whether the EHR could depend upon some other system component (e.g., operating system) or external service to meet the criterion. Given that many privacy and security functions and assurances are provided by the infrastructure in which an “EHR” operates, one might reasonably assume that the EHR itself would not need to provide basic, foundational security functions and assurances. Indeed, we believe that EHR technology should depend primarily upon infrastructure assurances and specialized security services, and that the EHR itself should provide only those security services that are specific to protecting the confidentiality, integrity, and availability of electronic health information. The Workgroup ultimately agreed that throughout our recommendations, we would use the term “EHR” to include the Complete EHR or EHR Module(s) submitted for certification, plus any infrastructure and third-party services that the EHR technology may rely upon to meet the criterion.
 - We see the integration of EHR, infrastructure, and specialized security products and services as key to protecting electronic health information, care quality, and patient safety. To enable the certification process to more effectively address security integration, we recommend that the ONC and NIST consider modifying the certification process so that each privacy and security certification criterion is treated as “addressable,” similar to how the implementation specifications in the HIPAA Security Rule are “addressable.” That is, to meet each security criterion, each Complete EHR or EHR Module submitted for certification would need to either:
 - a) Implement the required security functionality within the Complete EHR or EHR Module(s) submitted for certification; or
 - b) Assign the function to a third-party security component or service, and demonstrate how the certified EHR product, integrated with its third-party components and services, meets the criterion.
- ◆ Recommendations have been approved pending amended language concerning SHA-1 and SHA-2

S&I Framework Follow-up Discussion (Doug Fridsma, ONC)

- ◆ We are a year into standing up the activities within the S&I framework
 - We are looking at how to refine the process while remaining targeted, lean and agile
 - Had a meeting October 18-19: 234 attended
 - We have close to 9 initiatives
 - We have 885 registered users participating
- ◆ Transitions of Care Initiative
 - **Purpose:** The Transitions of Care (ToC) Initiative is focused on improving the electronic exchange of core clinical information among providers, patients, and other authorized entities in support of Meaningful Use and IOM-identified needs for improvement in the quality of care.
 - ToC Initiative has developed several critical outputs to enable interoperability:
 - **Clinical Information Model (CIM)** consisting of unambiguous, clinically-relevant definitions of the core data elements that should be included in care transitions
 - Over time, new elements can be added to support evolving needs
 - Reflective of real-world workflows and care transitions processes
 - **Clear guidance on the usage** of these core clinical elements in common care transitions scenarios

- Agreement on a **single standard** for clinical summary documents in support of Meaningful Use requirements
- Minimizes interoperability errors and streamlines patient care coordination
- **Implementer guidance** on vocabulary mapping as well as conversion tools to migrate existing implementations to the Consolidated CDA standard

Update on Metadata ANPRM – Public Comment (Steve Posnack, ONC)

- ◆ ONC received comments from:
 - Associations, EHR vendors, HIT Software Companies (11/51).
 - Infrastructure experts and Standard Development Organizations (2/51).
 - Providers, Pharmacy or Pharmacy Organizations, Hospitals and Health Plans (21/51).
 - Others including Policy Organizations, Individual Citizens and Government Entities (17/51).
- ◆ General Analysis
 - **General - Use of Metadata:** 48 of the 50 commenters supported use of metadata.
 - a) Many were opposed to federal regulations and wanted industry (SDOs) to set metadata standards.
 - b) 9 commenters specifically said that metadata standards are not ready to be included for Stage 2.
 - **General - Using CDA R2:** 16 out of 27 commenters supported use of HL7 CDA R2.
 - a) Of the 11 “no’s,” many were resistant to specifying CDA R2 as a standard and requested that regulations only specify the metadata elements and not architecture.
- ◆ Patient Identity – General
- ◆ **Commenters generally supported the patient identity data elements listed in the ANPRM but offered the following recommendations:**
 - **Name:** Require birth name, maiden name, and date ranges (*e.g., individuals can have several different last names from marriages/divorces, dates would be important for proper id*).
 - **Date of Birth:** Need to specify "month, day, year" format.
 - **Address** (current): 10/24 commenters who supported “address” as a metadata element stated that more detail must be provided before address is a useful metadata element (*without date ranges, address can be less reliable/useful*).
 - **Zip code** (current): 9/23 commenters supported “zip code” as a metadata element stated that more detail must be provided before it is a useful metadata element (*some stated that zip code should be changed to postal code to accommodate international addresses*).
 - **Additional Pt ID Elements:** 24/26 commenters stated that additional Pt ID elements are essential for accurate patient matching. A number of vendors stated that patient ID should NOT be part of data and that metadata should describe only the type of document in the package.
- ◆ Patient Identity – Additional Elements
 - **Additional metadata elements within the patient identity category suggested for inclusion:**
 - a) Gender (n=12)
 - b) Place of birth: (n=6) (city and state, or foreign country) is a data point that does not change over time.
 - c) Unique, voluntary patient identifier (n=3) /National patient ID (n=2)
 - d) Mother’s maiden name (n=4) or first name (n=2)
 - e) Birth order: (n=3) May be required to identify newborns, who may not yet have full demographic information available.
 - f) Race/ethnicity (n=3)
 - g) Previous address/zip with date ranges (n=2)

- h) Phone /email address (n=2)
- i) Insurance policy number (n=2)
- **Commenters suggested that the following patient identity elements should be considered for removal:**
 - a) Address: should be optional; of marginal additive value in making a positive patient identification and cannot be used with a high degree of certainty.
 - b) Zip code: not a good identity field as it is often inaccurately reported by patients or not known, and it may change over time as needed by the US Postal Service.
 - c) Name Prefix: changes routinely, and name prefix is not a contributor to unique identity, no added value.
 - d) Last 4 digits of SSN: consider as a secondary and not primary match criterion because it will not be unique. Consider using full SSN.
 - e) A majority of commenters (26/30) believe that if an individual lacks address information, then it would NOT be appropriate to include the institution's address.
- ♦ Provenance
 - **Additional Provenance Elements: 16/21 commenters stated that additional provenance elements are essential for accurate data linkage during queries.**
 - a) Specifically, commenters wanted additional data elements about:
 - Dates of service (n=6)
 - Actor and their credentials (n=5)
 - Author and their role (n=5)
 - Type of service performed (n=4)
 - Document type (i.e., consent, lab, summary doc) (n=2)
 - Document creation date/timestamp (n=3)
 - Source of the information (e.g., pt, family, provider, lab, etc) (n=2)
 - Commenters (n=8) stated that the digital signature should not be included as part of the metadata.
 - A majority of commenters recommended that time stamp, actor, and actor's affiliation be expressed in XML syntax rather than including in a digital certificate (n=17).
- ♦ Privacy Policy – General
 - Metadata should only describe the data set.
 - a) Privacy should be a separate layer from the metadata. Many commenters suggested looking into HITSP TP30.
 - Many commenters had concerns that detailed privacy tags would inadvertently divulge sensitive information.
- ♦ Privacy
 - **Policy Pointers:**
 - a) 19/28 commenters stated that the use of policy pointers would be problematic.
 - b) 11 commenters specifically stated that policy pointers should not be part of Stage 2 certification requirements.
 - Reasons given to **exclude** policy pointers in metadata:
 - a) The use of policy pointers is immature due to lack of necessary standards, infrastructure, and industry experience.
 - b) Policy persistence is an issue. Current policy pointer technology does not scale as data sets age or policies are updated.
 - c) Currently, privacy policies cannot be expressed in a computable fashion.
- ♦ Privacy Sensitivity Tags
 - 21/27 commenters supported the use of sensitivity tags.

- a) 11/21 yes's were conditional where commenters stated that more LOINC codes may not be accurate enough.
- Most commenters supported the use of LOINC, but also suggested SNOMED.
 - a) Many warned of value set being too granular and allowing inferences to be made.
 - Most commenters agreed with the HIT Standards Committee's recommendation against adopting an approach that would tag privacy policies directly to the data elements.
 - 8 commenters specifically stated that the ConfidentialityByInfoType value set should not be used. Instead they advocated for the use of ConfidentialityByAccessKind.
- ◆ Metadata Representation Structure
 - As stated previously, most commenters supported the use of HL7 CDA R2.
 - Some were concerned that changes proposed in the ANPRM to the CDA R2 header would be non-compatible.
 - A few commenters specifically stated that no representation structure should be proposed without pilot testing.
 - Several commenters asked that ONC specify only the metadata elements and not the representation structure.
 - A number of vendors asked ONC to consider XDS instead of HL7 CDA R2.
- ◆ Implementation Consideration/Use Cases
 - Commenters were divided regarding the level of difficulty in designing EHR technology to assign metadata for MU Stage 2.
 - a) Some believed that EHR technology is mature enough to include this capability.
 - b) Others felt strongly that not enough progress has been made to include this capability.
 - Additional analysis and real-world testing is needed before proposing metadata standards to support Stage 2.
 - Other potential use cases identified for metadata included: Public health, research queries/clinical trials, disease registries, transitions of care, patient engagement, and billing purposes.
- ◆ Additional Standards and other Considerations
 - Most commenters believed that additional categories of metadata are not necessary other than patient ID, provenance and privacy.
 - a) Although as presented, most commenters felt that standards to support privacy metadata were either unavailable or immature.
 - Several commenters pointed out that a metadata element could be used for patient ID, provenance, and privacy.
 - a) They are not mutually exclusive to one category.
 - b) Metadata categories are better described as uses of metadata.
 - Some commenters recommended that ONC clearly define expectations and requirements for managing changes to metadata elements (such as name) over time.