Health IT Standards Committee
A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

Transport and Security Standards Workgroup

Certification NPRM Comments Package

Dixie Baker, Chair
Lisa Gallagher, Co-Chair

May 20, 2015

TSS WG Members

- **Dixie B. Baker**, Chair, Martin, Blanck, and Associates
- **Lisa Gallagher**, Co-Chair, Healthcare Information and Management Systems Society
- **Jeff Brandt,** Member, Consultant
- **Brian Freedman,** Member, Security Risk Solutions, Inc.
- **John Hummel,** Member, Tahoe Forest Hospital District
- **LeRoy Jones,** Member, GSI Health
- **Boban Jose,** Member, RelayHealth
- **Peter Kaufman,** Member, DrFirst
- **Steven Lane,** Member, Sutter Health
- **Aaron Miri,** Member, Children's Medical Center
- **Scott Rea,** Member, DigiCert
- **Jason Taule,** Member, FEi Systems
- **Sharon F. Terry**, Member, Genetic Alliance
- **Jeremy Maxwell,** Staff Lead, HHS/ONC

Agenda

1. Standards Readiness for Inclusion in Certification – Summary
2. Revised approach to certifying Health IT Module against Privacy and Security criteria
3. Questions re Privacy and Security Criteria
4. Other questions

Agenda

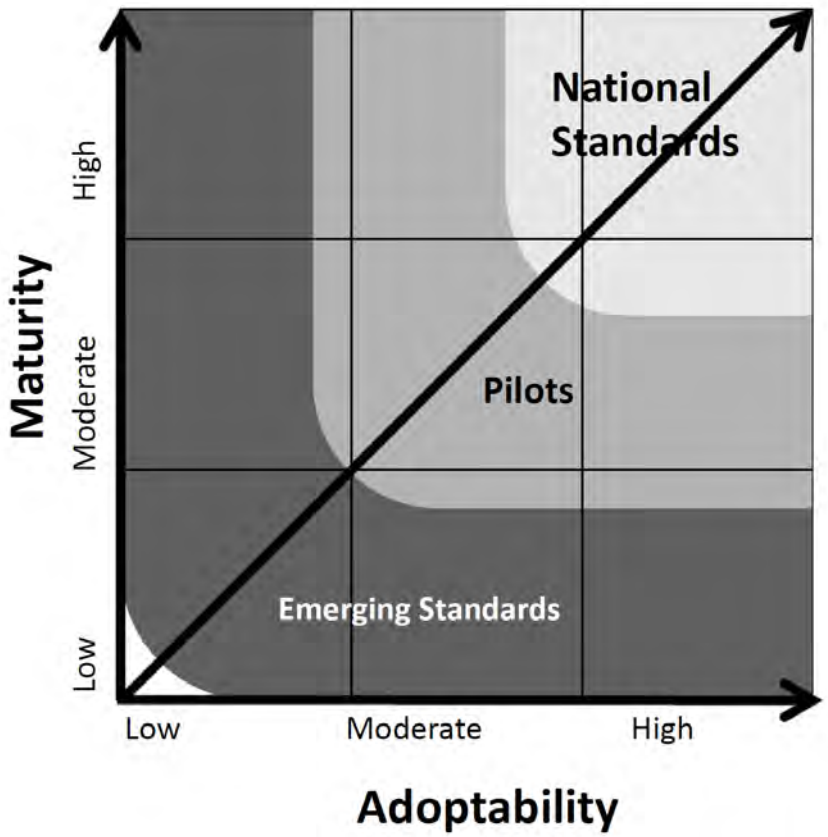
1. **Standards Readiness for Inclusion in Certification – Summary**
2. Revised approach to certifying Health IT Module against Privacy and Security criteria
3. Questions re Privacy and Security Criteria
4. Other questions

HITSC Readiness Evaluation and Classification Criteria for Technical Specifications

The Metrics the HITSC has adopted for helping to determine when a technology specification is ready to become a national standard.

Maturity Criteria:
- Maturity of Specification
- Maturity of Underlying Technology Components
- Market Adoption

Adoptability Criteria:
- Ease of Implementation and Deployment
- Ease of Operations
- Intellectual Property



Source:
http://jamia.oxfordjournals.org/content/jaminfo/early/2014/12/17/amiajnl-2014-002802.full.pdf?%2520ijkey=8oAq1ZTZyQ6edqC&keytype=ref

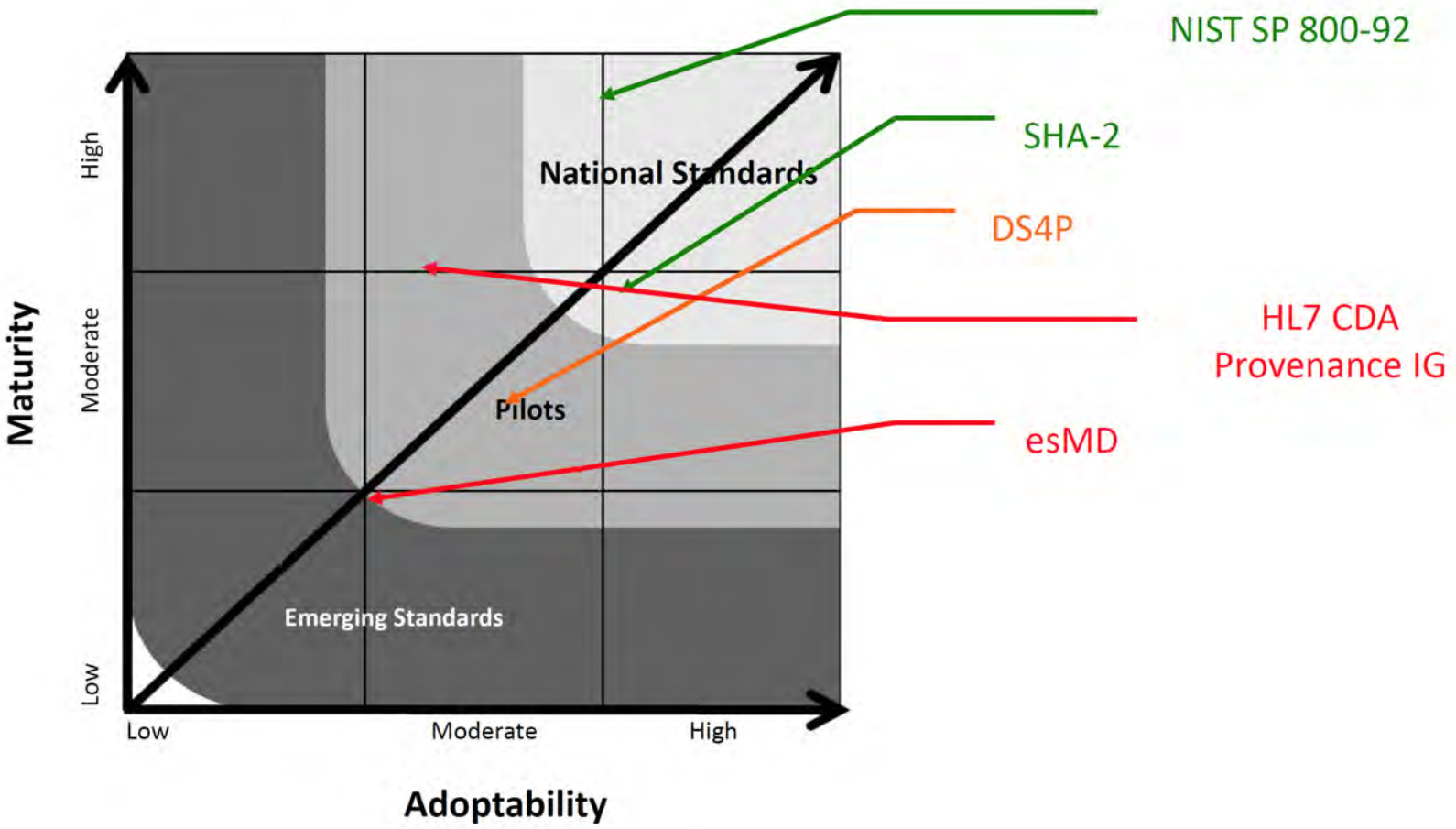
Standards Readiness for Inclusion in Certification

Standard	Ready (y/n)	Notes / path forward
SHA-2 (Secure Hash Algorithm)	Yes	Recommend ONC replace SHA-1 with SHA-2 in 2015 Edition
Data Segmentation for Privacy (DS4P)	No	Has been piloted, and beginning trial implementations in EHR products – resulting in concerns that need to be addressed. Important in that enables data exchange where none has been possible, but not ready to become a standard for certification
HL7 IG for CDA Release 2: Data Provenance, Release 1 (US Realm) (DSTU)	No	Encourage ONC to support continued piloting, use, and refinement of HL7 Provenance IG and FHIR Provenance-Content specification

Standards Readiness for Inclusion in Certification, continued

Standard	Ready (y/n)	Notes / path forward
Electronic Submission of Medical Records (esMD)	No	Applaud significant work since 2013: digital signature standard is consistent with DEA. Encourage ONC to pursue other levers to support further development and piloting
NIST 800-92 (*Guide to Computer Security Log Management*)	Yes	Recommend ONC add this standard to require that certified HIT be capable of recording an audit trail of all security-relevant events

HITSC Readiness Evaluation and Classification Criteria for Technical Specifications



Agenda

1. Standards Readiness for Inclusion in Certification – Summary
2. **Revised approach to certifying Health IT Module against Privacy and Security criteria**
3. Questions re Privacy and Security Criteria
4. Other questions

Health IT Module Certification Requirements: Privacy and Security

- NPRM proposes a new approach for privacy and security (P&S) certification
  - HIT Modules presented for certification will be certified against all of and only those security and privacy criteria identified as relevant to the functionality provided (e.g., clinical, care coordination) using either of two approaches:
    - Technically demonstrate, or
    - System documentation

Health IT Module Certification Requirements: Privacy and Security

Comment:

- Agree with new approach to P&S certification
- Recommend adding P&S criteria:
  - Clinical Module: add Integrity criterion
    - Involves transmissions (lab order compendium; formulary benefit file)
  - Care Coordination Module: add Amendments criterion
    - Support patient requested amendments
  - Design and Performance Module, API criterion: add (1) authentication, access control, and authorization; (2) Auditable events and tamper-resistance; and (8) Integrity

Agenda

1. Standards Readiness for Inclusion in Certification – Summary
2. Revised approach to certifying Health IT Module against Privacy and Security criteria
3. **Questions re Privacy and Security Criteria**
4. Other questions

Auditable Events and Tamper-Resistance

- NPRM proposes making change in user privileges auditable
- Should certain critical events be enabled at all times?

Comment:

- All security-relevant events should be auditable. A change in user privileges is security-relevant and therefore auditable
  - Add certification criterion stating that certified HIT should be capable of recording an audit trail of all security-relevant events
  - Add NIST SP 800-92, sections 2.1.2 and 2.1.3, as standard for specification of auditable events, in addition to ASTM E2147-01
- What to audit is a risk management decision
- Ability to disable audit log? Yes.
  - Recommend no change from 2014 Final Rule

Automatic Access Time-Out

- NPRM proposes to require a Health IT Module to … "automatically stop user access to health information after a predetermined period of inactivity" and "require user authentication in order to resume or regain access that was stopped"
- Comment
  - Suggested language change: "Automatically terminate access to protected health information after a configurable period of inactivity, and reinitiate session upon re-authentication of the user."

End-User Device Encryption

- NPRM proposes to update the encryption standard to the October 2014 release of FIPS 140-2, Annex A

Comment:

- Agree with proposed change
- In addition, suggest adding reference to FIPS 140-2, Annex A (which includes *Guideline for Transport Layer Security (TLS))*, to support proposed new certification criteria for "application access" for:
  - Patient Engagement, and
  - Common Clinical Data Set

Integrity

- NPRM proposes that testing against criterion focus on receipt of a summary record
- NPRM seeks guidance on when the SHA-1 integrity standard should be changed to SHA-2

Comment:

- Agree with change in testing approach
- Agree with proposal to move to SHA-2 in the 2015 Edition

Agenda

1. Standards Readiness for Inclusion in Certification – Summary
2. Revised approach to certifying Health IT Module against Privacy and Security criteria
3. Questions re Privacy and Security Criteria
4. **Other questions**

Data Segmentation for Privacy (DS4P)

- ONC proposes to adopt two new certification criteria that would focus on the capability to separately exchange and track ("segment") sensitive health information
  - Data Segmentation for Privacy: Send
  - Data Segmentation for Privacy: Receive

Comment:

- DS4P implementation is beyond pilot stage, and large vendors are now experimenting with its implementation – reporting needs for further refinement
- DS4P enables exchange of data that currently are not being exchanged – so important that piloting and implementations continue to progress
- Recommend that ONC continue to support and encourage trial implementations of DS4P in EHR technology to help accelerate specification refinement and adoption

Electronic Submission of Medical Documentation (esMD)

- NPRM proposes the adoption of esMD to support the submittal of C-CDA documents to CMS
  - Creation of C-CDA document
  - Use of W3C XML Advanced Electronic Signatures (XAdES) standard to digitally sign content, assuring both data integrity and non-repudiation
  - Creation and embedding of digital signatures applied to segments within C-CDA documents
  - Creation of “external digital signature” and transmittal of signed document

Electronic Submission of Medical Documentation (esMD), continued

Comments:

- Significant progress since August 2013 presentation to HITSC
  - Digital signature consistent with DEA standard
  - Capability can be provided by module natively or through external interface
- Tied to C-CDA Release 2; lacks wide adoption
- Not ready to become national standard
- Recommend ONC support pilots to advance refinement, implementability, and adoption to accelerate readiness

C-CDA Data Provenance

ONC seeks comment on the following:

- Maturity and appropriateness of HL7 Implementation Guide (IG) for the tagging of health information with provenance metadata in connection with C-CDA
- Usefulness of the HL7 IG in connection with certification criteria, such as Transitions of Care and View, Download, and Transmit certification criteria

Comment

- HL7 currently working collaboratively on two different provenance specifications – HL7 Provenance IG and FHIR Provenance-Content specification
- Neither specification is ready to be adopted as a national standard
- Data provenance is significant component of data integrity – TSSWG encourages ONC to follow and support the development and piloting of these specifications