Health IT Standards Committee

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

Transport and Security Standards Workgroup

Interoperability Roadmap Comments Package

Dixie Baker, Chair
Lisa Gallagher, Co-Chair

April 22, 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. Section E
   - Ubiquitous, Secure Network Infrastructure
2. Section F
   - Verifiable identity and authentication of all participants
3. Section G
   - Consistent representation of permission to collect, share and use identifiable health information
4. Interoperability Roadmap Critical Actions

Comments – Section E

Ubiquitous, secure network infrastructure

Enabling an interoperable, learning health system requires a stable, secure, widely available network capability that supports vendor-neutral protocols and a wide variety of core services.

Section E – Ubiquitous, secure network infrastructure

E1(a). What should the federal government (specifically) focus on first to move towards a uniform approach to enforcing cybersecurity in healthcare (keeping HIPAA and CEHRT Rules in mind and possible new cybersecurity legislation)?

The Transport and Security Standards Workgroup (TSS WG) recommends that ONC partner with the National Institute of Standards and Technology (NIST), the Office of Civil Rights (OCR), other federal agencies, and industry stakeholders in several ways to enable a uniform approach to enforcing cybersecurity in healthcare.

Section E – Ubiquitous, secure network infrastructure, continued

E1(a) – Continued

- First, ONC should work to advance a consistent trust framework across the health IT ecosystem. Such a trust framework should allow for diversity in organizational policy, while enabling a foundational basis for mutual trust among organizations.

- Second, ONC should endorse a set of appropriate baseline security controls that are uniformly applied to health IT technologies that enter the ecosystem.

Section E – Ubiquitous, secure network infrastructure, continued

E1(a) – Continued

- Third, ONC should work with industry to accommodate a diversity of emerging health IT technologies across infrastructures within the health IT ecosystem. Health IT infrastructures must be flexible, in that they should permit any certified health IT solution to operate within the ecosystem.

- Fourth, ONC should provide guidance on proper governance in cybersecurity, which is essential for building trust and security throughout the ecosystem.

- Finally, the ONC should bring together federal, state, and industry stakeholders to address the goal of reducing variations in cybersecurity enforcement.

Section E – Ubiquitous, secure network infrastructure, continued

E1(b). Are there frameworks, methodologies, incentive programs, etc. that the healthcare industry has not, but should, consider?

ONC should consider the following in further establishing trust across the health IT ecosystem:

- First, ONC should consider including the "Trustmark Framework" developed in a NIST / National Strategy for Trusted Identities in Cyberspace (NSTIC) pilot, PCI Security Standards, and the ISO 27000 series as possible frameworks for establishing electronic trust among healthcare organizations across the Internet.
- Second, cybersecurity needs to be considered for both enterprises and for interconnections among enterprises.

Section E – Ubiquitous, secure network infrastructure, continued

E1(b) – Continued

- Third, the healthcare industry needs a minimum set of standards and metrics for measuring the strength of security protections. A number of "minimum standard sets" exist and can be drawn from. These include, but may not be limited to: OCR's minimum standards for control areas, the Certification Authority Browser (CA/B) Forum Baseline Requirements, and the questions asked by cybersecurity insurance companies and financial auditors.

- Fourth, the existing security control frameworks (including NIST's cybersecurity framework) should be considered for alignment and guidance when gaps occur.

Section E – Ubiquitous, secure network infrastructure, continued

E2. Are there other gaps (aside from lack of policies and guidance for implementing encryption) in technology and standards for encryption?

ONC should work with OCR, other federal partners, and industry stakeholders to address the following issues related to technology and standards for encryption.

- First, ONC should provide guidance on encryption key lifecycle management.
- Second, ONC should provide guidance on a method for encryption key escrow recovery.

Section E – Ubiquitous, secure network infrastructure, continued

E2 – Continued

- Third, ONC should publish guidance on key oversight and authorization, addressing the people or entities that maintain access to encryption keys.
- Finally, ONC should also consider providing guidance on a minimum set of circumstances in which encryption should be used to secure data (i.e., medical devices, systems, and software).

Comments – Section F

Verifiable identity and authentication of all participants

Legal requirements and cultural norms dictate that participants be known, so that access to data and services is appropriate. This is a requirement for all participants in a learning health system regardless of role (individual/patient, provider, technician, etc.)

Section F – Verifiable identity and authentication of all participants

F1. What ID proofing and authentication standards, policies, and protocols can we borrow from other industries? Is healthcare that different from banking, social media, or e-mail?

- Yes, healthcare is "that different." Although good cybersecurity best practices can be applied similarly across different industries, ONC should acknowledge that because of the sensitivity and criticality of data used in the healthcare industry, and the need for convenient access to data, sometimes in emergency circumstances, healthcare is notably different from banking, social media and email. Credit cards can be replaced, and new e-mail accounts can be generated, but deeply personal genetic or treatment information cannot be replaced or recalled once it is disclosed. Some harms may be irreparable.

Section F – Verifiable identity and authentication of all participants, continued

F1 – Continued

- Many security protections (e.g., access control, audit, digital signature) are dependent upon user identity, and for this reason, health information requires a high level of assurance in the processes and mechanisms used for identity proofing and authentication.
- ONC – together with OCR, other federal partners, and industry stakeholders – should continue to support the National Strategy for Trusted Identities in Cyberspace (NSTIC) program and to draw from existing pilots, where applicable.
- ONC should support NIST's effort to update SP 800-63 and to help assure its applicability to and utility for healthcare use cases.

Section F – Verifiable identity and authentication of all participants, continued

F1 – Continued

- ONC should provide guidance on the use of third-party identity proofing services, including trusted Internet identities used by individuals for everyday life activities such as banking, social media and shopping.
- Such guidance should affirm that the use of such third-party Internet identities should be contingent on their use of high-assurance methods for identity verification, consistent with evolving healthcare laws and regulatory requirements.

Comments – Section G

Consistent representation of permission to collect, share and use identifiable health information

Though legal requirements differ across the states, nationwide interoperability requires a consistent way to represent an individual's permission to collect, share and use their individually identifiable health information, including with whom and for what purpose(s).

Section G – Consistent representation of permission to collect, share and use identifiable health information

G1. What standards should we put forward in the 2016 standards advisory for basic choice?

Today's "standard" for basic choice is a paper document that is hand-signed by the patient. We appreciate ONC's recognition of the limited utility and scalability of this model in electronic exchange, and we share ONC's desire to identify open standards for electronically capturing, representing, exchanging, and interpreting patient consent.

Section G – Consistent representation of permission to collect, share and use identifiable health information, continued

G1 – Continued

Full end-to-end electronic capture, representation, exchange, and interpretation of patient consent is technologically possible and currently used in limited circumstances. However, we know of no mature standards that are widely used to electronically capture or represent patient consent decisions. Various efforts are underway, including work by Oasis and HL7, and ONC should continue to monitor these developments.

Section G – Consistent representation of permission to collect, share and use identifiable health information, continued

G2. How much work should ONC be doing on other standards while clarifying permitted uses? If standards development needs to be done, what should we be working on (DS4CDS v. DS4P v. something else)?

- Rather than commit resources to creating new standards, ONC should monitor and, where appropriate, engage in existing efforts to capture consent electronically. This includes the development of emerging consumer consent technologies. We recognize electronic (computable) consent is valuable for the future of health IT.

Section G – Consistent representation of permission to collect, share and use identifiable health information, continued

G2 - Continued

- ONC should also provide guidance that defines computable, discrete data fields needed for negotiating patient consent and access to health information. Common semantics for discrete data fields would further assist in determining whether the protected health information or personally identifiable information should be shared.
- ONC should continue to monitor SAMHSA pilots and the application of DS4P technology, and derive lessons learned from those efforts.

Comments to Interoperability Roadmap Critical Actions

Sections E and G

Comments – Section E Critical Actions

E1. Cybersecurity

(2) ONC will coordinate with the Office of the Assistant Secretary for Preparedness and Response (ASPR) on priority issues related to cyber security for critical public health infrastructure.

- Replace "critical public health infrastructure" with "critical health infrastructure" (which includes, but is not limited to, "public" health infrastructure).

- In considering the cybersecurity needs of the nation's health infrastructure, availability and resiliency, data integrity, and confidentiality should all be considered as part of the critical components for organizational preparedness and response.

- In addressing issues related to preparedness and disaster recovery for cyber attacks, ONC should consider learning from, and building upon, the National Disaster Medical System (NDMS). Today, the NDMS public health system works offline and has been tested in prior public health emergencies.

Comments – Section E Critical Actions, continued

E1. Cybersecurity, continued

(3) HHS will continue to support, promote and enhance the establishment of a single health and public health cybersecurity Information Sharing and Analysis Center (ISAC) for bi-directional information sharing about cyber threats and vulnerabilities between private health care industry and the federal government.

- We support this action. For the out years, ONC should provide guidance and reference implementations for enabling healthcare organizations to electronically consume threat information to minimize the risk and impact of cyber-attacks.

Comments – Section G Critical Actions

G4. Technical standards for basic choice

(3) Technology developers implement technical standards and implementation guidance for consistently capturing, communicating and processing individual choice. Adoption has begun, with 5% of exchangers using the standards regularly.

- ONC should consider changing this from "2018-2020" to "2015-2017".

Comments – Section G Critical Actions, continued

G4. Technical standards for basic choice, continued

(4) Technology developers implement technical standards and implementation guidance for consistently capturing, communicating and processing individual basic choice. Adoption continues, with a majority of exchangers using the standards regularly.

- Due to the advancements in genomics, ONC should consider changing this from “2021-2024” to “2018-2020”.

Comments – Section G Critical Actions, continued

G4. Technical standards for basic choice, continued

(5) Basic choice standards are used widely to electronically capture individuals' desire to have their health information included in research.

- Since this is happening already, ONC should consider changing this from "2021-2024" to "2015-2018".

References

Entity	URL
NSTIC	http://www.nist.gov/nstic/
ISO	http://www.iso.org/iso/home.htm
NIST / NSTIC Trust Framework	https://trustmark.gtri.gatech.edu
CA/B Forum	https://cabforum.org
NIST Cybersecurity Framework	http://www.nist.gov/cyberframework
NDMS	http://ndms.fhpr.osd.mil