Health IT Standards Committee

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

Transport & Security Standards Workgroup

Update on Interoperability Roadmap Comments

Sections E, F, and G

Dixie Baker, chair
Lisa Gallagher, co-chair

March 18, 2015

Charge to Transport and Security Workgroup

Workgroup	Transport and Security Standards
Section E: Secure Network Infrastructure	1) Cybersecurity: 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)? b) Are there frameworks, methodologies, incentive programs, etc. that the healthcare industry has not, but should, consider? 2) Encryption: Are there other gaps (aside from lack of policies and guidance for implementing encryption)in technology and standards for encryption?
Section F: Identity and Authentication	What ID proofing and authentication standards, policies, and protocols can we borrow from other industries? Is healthcare *that* different from banking, social media, or email?
Section G: Consent	What standards should we put forward in the 2016 standards advisory for basic choice? 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 vs DS4P vs something else)?

TSS WG: Tasks & Dates

Date	Task
Feb 24	WG discussion on Section E
Mar 11	WG discussion on Section F & G
Mar 18	**HITSC Meeting**
Mar 25	Additional discussion, final review of comments
April 6	Complete comments and prepare for submission

Draft Comments for Discussion – Section E

Roadmap Section E Summary: Cybersecurity, continued

1a) 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)?

DRAFT Response:

- The Transport and Security Standards Workgroup (TSS WG) recommends that ONC partner with NIST, OCR, other federal agencies, and industry stakeholders in several ways to address a uniform approach to enforcing cybersecurity in healthcare.
- First, ONC should work to advance a consistent trust framework across the health IT ecosystem.
- Second, ONC should endorse a set of appropriate baseline security controls that are uniformly applied to all health IT technologies that enter the ecosystem.
- 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.

Roadmap Section E Summary: Cybersecurity

1b) Are there frameworks, methodologies, incentive programs, etc. that the healthcare industry has not, but should, consider?

DRAFT Response:

- Trust is integral in building a secure health IT ecosystem. The National Strategy for Trusted Identities in Cyberspace (NSTIC) Trustmark, PCI, and ISO should be considered as possible frameworks for establishing electronic trust among healthcare organizations across the Internet.
- Cybersecurity needs to be considered for both enterprises and for interconnections among enterprises.
- 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 CAB-forum Baseline Requirements, and the questions asked by cybersecurity insurance companies and financial auditors.
- Additionally, the existing security control frameworks (including NIST's cybersecurity framework) should be considered for alignment and guidance when gaps occur.

*http://www.nist.gov/cyberframework

Roadmap Section E Summary: Encryption

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

DRAFT Response:

- ONC should work with OCR, other federal partners, and industry stakeholders to address the following three 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.
- Finally, ONC should publish guidance on key oversight and authorization, addressing the people or entities that maintain access to encryption keys.
- ONC should also consider providing guidance on a minimum set of encryption requirements for health IT (i.e., medical devices, systems, and software) used to store and access protected health information.