Health IT Standards Committee

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

Transport & Security Standards Workgroup

User Authentication Recommendations

December 10, 2014

Background - HITPC Recommendations

Health IT Policy Committee (HITPC) Privacy and Security Tiger Team Recommendations re *Authentication* (2012, 2013)

- Move toward multifactor authentication (National Institute of Standards and Technology (NIST) level of assurance (LOA) 3 for provider remote access of protected health information (PHI)
- Continue to identity proof providers in compliance with the Health Insurance Portability and Accountability Act (HIPAA)
- Continue to be informed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative
- Engage with NSTIC initiative to help align direction in consumer identity-proofing, authentication, and the use of third-party credentials with the needs of the healthcare industry

Recap of Relevant TSSWG Presentations

- Trustmarks
- OpenID Connect (authentication)
- OAuth 2.0 (authorization)
  - Related profiles: BB+ and User Managed Access
- NIST new directions in identity management

2014 Edition Authentication Criterion

§ 170.314 2014 Edition electronic health record certification criteria.

(d) Privacy and security.

(1) Authentication, access control, and authorization.

(i) Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed;

Recommendations (1 of 3)

- To strengthen the authentication currently certified in EHR technology, the TSSWG recommends adding the following criteria:

  (ii) Continuously protect the integrity and confidentiality of information used to authenticate users, using the standard specified in §170.210(a)(1) of the 2014 Edition EHR Standards, Implementation Specifications, and Certification Criteria.

  (iii) If passwords are used for user authentication, accept only passwords that meet the guessing entropy guidelines set forth in Appendix A of NIST 800-63-2.

Recommendations (2 of 3)

- To enable EHR technology to be certified for having implemented multi-factor authentication, the TSSWG recommends adding the following certification criterion:
  - Restrict access to the system, or to one or more individual functions within the system (e.g., prescribing controlled substances), to only those individuals who have presented at least two of the following three forms of authentication -- knowledge of a secret (e.g., password), possession of a physical object (e.g., hard token or smartcard), a biometric (e.g., fingerprint).

Recommendations (3 of 3)

The TSSWG further recommends that the ONC:

- Support NIST effort to revamp NIST Special Publication 800-63-2 (Electronic Authentication Guideline)
  - Closely follow move from LOA to componentized trust
  - Recommend appropriate identity-proofing for query-based access
- Consider Data Segmentation for Privacy (DS4P) for authorizing access to behavioral data (TSSWG will address later in the work plan)
- Track development and piloting of User Managed Access (UMA) profile of OAuth 2.0 as potential standard for consumer consent