Privacy and Security Tiger Team

Trusted Identity of Providers in Cyberspace

Follow-Up Recommendations

September 6, 2012

Tiger Team Members

- **Deven McGraw, Chair**, Center for Democracy & Technology
- **Paul Egerman, Co-Chair**
- **Dixie Baker**, SAIC
- **Dan Callahan,** Social Security Administration
- **Neil Calman**, Institute for Family Health
- **Carol Diamond**, Markle Foundation
- **Judy Faulkner**, EPIC Systems Corp.
- **Leslie Francis**, University of Utah; NCVHS
- **Gayle Harrell**, Consumer Representative/Florida
- **John Houston**, University of Pittsburgh Medical Center
- **Alice Leiter**, National Partnership for Women & Families
- **David McCallie**, Cerner Corp.
- **Wes Rishel**, Gartner
- **Latanya Sweeney**, Carnegie Mellon University
- **Micky Tripathi**, Massachusetts eHealth Collaborative

Reminder – Scope of Discussion

- Focus is on "trusted identity“ – identity proofing for the issuance of credentials to be used for authenticating the identity of providers
  - Did not address trusted access, authorization
  - Focused on provider users; patient access to be addressed at a later time
  - Question we addressed is: “are you whom you claim to be?”, with a sufficient level of assurance based on the intended purpose for the exchange of clinical data

Recommendations to the HIT Policy Committee (1/3)

1. By Meaningful Use Stage 3, ONC should move toward requiring multi-factor authentication (meeting NIST Level of Assurance (LOA) 3) for remote access to protected health information. Remote access includes the following scenarios:
   A. Access from outside of an organization's/entity's private network.
   B. Access from an IP address not recognized as part of the organization/entity or that is outside of the organization/entity's compliance environment.
   C. Access across a network any part of which is or could be unsecure (such as across the open Internet or using an unsecure wireless connection).

Recommendations to the HIT Policy Committee (2/3)

2. Organizations/entities, as part of their HIPAA Security risk analysis, should identify any other access environments that may require multiple factors to authenticate an asserted identity.
3. Organizations/entities should continue to identity proof provider users in compliance with HIPAA. (Tiger Team did not see a need to establish identity proofing requirements for different types of access scenarios).
4. Such policies should extend to all clinical (provider) users accessing/exchanging data remotely.
5. Technology options for authentication continue to evolve; ONC should continue to monitor and update policies as appropriate to reflect improved technological capabilities.

Recommendations (3 of 3)

6. ONC's work to implement this recommendation should continue to be informed by NSTIC and aim to establish trust within the health care system, taking into account provider workflow needs and the impact of approaches to trusted identity proofing and authentication on health care on health care quality and safety.
   - For example, NSTIC also will focus on the capability to pass along key attributes that can be associated with an identity. The capability to pass key attributes – e.g., valid professional license – may be critical to facilitating access to data.
7. ONC should consult with NIST about future iterations of NIST 800-63-1 to identify any unique needs in the healthcare environment that must be specifically addressed.

Backup Slides

800-63 Authentication Requirements

LOA2	LOA3
Single factor	Multi-factor
NIST LOA2 Identity Proofing	NIST LOA3 Identity proofing
Approved cryptographic techniques required	Approved cryptographic required for all operations
Must prove control of token	Must first unlock token by means of password or biometric in addition to prove control of token
Eaves dropper, on-line guessing, session hijacking prevented, weakly resistant to man-in-the-middle	Eavesdropper, replay, on-line guessing, session hacking, verifier impersonation prevented. Man-in-the-middle attacks prevented when combined with FIPS 140-2 compliant tokens
LOA3/LOA 4 Multi-factor may be used	Minimum of two factors required :Examples: shared secret, mobile one-time- password (OTP) application, PKI, USB token, credit card password tokens, RFID or blue tooth token

Use of Biometrics for Authentication

- NIST 800-63-1 is for remote applications, i.e., when no attendant is watching the users trying to log on to a system
- Security/privacy issues with biometrics
  - Biometrics are not secrets and may be spoofed relatively easily and inexpensively
  - Anti-spoofing techniques are not mature enough to write a spec for or test for performance
  - Data at rest can be encrypted but traditional cryptography cannot be used to protect patient's data to do matching, in the same way that password authentication is done
- Although ONC and other NIST-assisted efforts are underway to address these issues, solutions may be some time off