Health IT Policy Committee

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

September 26, 2012

Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Mostashari:

The HIT Policy Committee (Committee) gave the following broad charge to the Privacy & Security Tiger Team (Tiger Team):

Broad Charge for the Privacy & Security Tiger Team:
The Tiger Team is charged with making short-term and long-term recommendations to the Health Information Technology Policy Committee (HITPC) on privacy and security policies and practices that will help build public trust in health information technology and electronic HIE, and enable their appropriate use to improve healthcare quality and efficiency, particularly as related to ARRA and the Affordable Care Act (ACA) which mandates a number of duties to the Office of the National Coordinator (ONC) relative to privacy and security.

This letter provides recommendations to the National Coordinator, Department of Health and Human Services (HHS) on provider authentication for exchange of clinical data.

Background
ONC requested that the Tiger Team consider identity management and the ongoing National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative and its applicability to physician authentication. On April 18, 2011, the Policy Committee endorsed previous recommendations from the Tiger Team on EHR-user (provider) authentication, which focused on:

- Digital certificates, issued at an entity level, to provide a "high" degree of assurance, with each entity credentialing its individual provider users. This approach was intended to assure a trusted "machine to machine" transfer of protected health information.
- Individual-level credentials for accessing information across a network (such as NwHIN) should be issued at a level higher than just user name and password [Level of Assurance (LOA) 2]. At that time the Tiger Team was not prepared to recommend LOA 3 due to uncertainties about the burden on healthcare entities.

Recognizing the evolving nature of the environment, the recommendations also called for re-assessment of policy for consistency with related efforts. Given NSTIC progress and the recent update of NIST's *Electronic Authentication Guidelines* (NIST Special Publication 800-63-1) in December 2011, the Tiger Team felt such a re-assessment was timely.

The Tiger Team's focus was on "trusted identity," that is, identity proofing for the issuance of credentials to be used for authenticating the identity of provider users in the context of electronic health information exchange. The Tiger Team did not address trusted *access* or *authorization* by provider users. In summary, the question addressed was: "Are you whom you claim to be?" with a sufficient level of assurance based on the intended purpose for the exchange of clinical data. To inform its deliberations, the Tiger Team and the HITSC's Privacy and Security Work Group held a joint hearing on "Trusted Identities of Providers in Cyberspace" on July 11, 2012. In this hearing, the Tiger Team heard testimony from a wide variety of witnesses including NIST, federal agencies, and healthcare entities with experience in provider user identity proofing and authentication.

It should be noted that the focus of these deliberations was exclusively on provider user authentication. However, the Tiger Team recognizes that patient/consumer authentication (for example, to access Stage 2 view/download and transmit functionalities) is also an important issue and plans to address this in a public hearing in Fall 2012 and a series of upcoming meetings.

Recommendations

Based on the testimony at the hearing, the Tiger Team observed that the focus of identity assurance generally seems to be shifting from the entity/organization level to the individual level. In addition, it appears that under NIST 800-63-1 Level of Assurance 3 (LOA 3), multi-factor authentication is more feasible (with more options for the second factor), and is consistent with the direction the industry is heading. At the September 6, 2012 HIT Policy Committee meeting, the Tiger Team presented their new recommendations on provider authentication, which replace its previous recommendations on this issue. The Committee deliberated on the findings and approved the recommendations below for transmittal to the National Coordinator.

1. By Meaningful Use Stage 3, ONC should move toward requiring multi-factor authentication (meeting NIST Level of Assurance (LOA) 3) by provider users to remotely access 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).
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.
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.

We appreciate the opportunity to provide these recommendations on provider authentication and look forward to discussing next steps.

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee