Health IT Policy Committee

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

May 3, 2013

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 patient identity proofing and authentication for access to patient portals and the view, download, and transmit functions required under Stage 2 Meaningful Use.

Background
In considering its recent recommendations on provider user identity proofing and authentication, the Tiger Team recognized that patient/consumer identity proofing and authentication (for example, to access Stage 2 view/download and transmit functionalities) was also an important issue and made plans to address this issue separately. The Tiger Team had previously considered patient authentication and on April 18, 2011, the Policy Committee endorsed the following recommendation:

- Providers should require at least a user name and password to authenticate patients.
  - This single-factor authentication should be a minimum. Providers may want to offer their patients additional security (such as through additional authentication factors) or provide such additional security for access to particularly sensitive data.
  - In setting authentication requirements, providers should also be mindful of guidelines for identification and not set requirements so high that patients are discouraged or cannot meaningfully participate.

To inform its deliberations, the Tiger Team and the HIT Standards Committee's (HITSC) Privacy and Security Work Group held a joint hearing on "Trusted Identities of Patients in Cyberspace" on November 27, 2012. In this hearing, the Tiger Team heard testimony from a wide variety of witnesses including

federal and state agencies, healthcare entities with experience in patient identity proofing and authentication, and representatives from other industries that make potentially sensitive information available to consumers on-line. The hearing focused on the following issues: (1) the challenges faced in the use of patient portals, and patient authentication and identity proofing, (2) current approaches used by provider entities, (3) approaches used in other industries, and (4) emerging approaches, which may be future solutions. In addition, the Tiger Team gathered information from the public through the HIT Policy Committee blog.

Recommendations

At the January 8, 2013 HIT Policy Committee meeting, the Tiger Team presented additional recommendations on patient identity proofing and authentication. These recommendations, which build on the previous ones cited above, are provided in terms of best practices. The Privacy and Security Rules already require identity proofing and authentication for anyone accessing PHI from a covered entity or business associate. However, these requirements do not contain a great deal of detail on how to implement these requirements. Consequently, the Tiger Team concluded that rather than a change to the law or other requirements, education to providers in the form of best practices was needed. Further, these best practices should be informed over time by the considerable innovation occurring in this space.

The HIT Policy Committee deliberated on these findings and approved the recommendations below for transmittal to the National Coordinator.

Overarching Recommendation 1: ONC should develop and disseminate best practices for identity proofing and authentication for patient access to portals (MU2 view, download, and transmit capability); such best practices should be disseminated to eligible professionals (EPs), eligible hospitals (EHs), and critical access hospitals (CAHs) sufficiently in advance of the onset of Stage 2 to enable planning.

- ONC should disseminate these best practices to providers through the Regional Extension Centers (RECs) and through other means to ensure wide distribution.
- These best practices should also be disseminated to vendors.

Recommendation 2: Such best practices should be consistent with the following overarching principles:

- Protections should be commensurate with risks.
- Approaches should offer simplicity and ease of use for patients and be consistent with what patients are willing and able to do.
- Solutions should provide flexibility in the methods offered; ”one size does not fit all.”
- Approaches should leverage solutions in other sectors, such as online banking.
- Solutions should be accompanied by education that make these processes transparent to the patient.
- Approaches taken should build to scalable solutions (e.g., greater use of voluntary secure identity providers such as those envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC)).
- Solutions need to evolve over time as technology changes

Discussion on Best Practices

Based on the results of the patient authentication hearing and posts on the blog, the Tiger Team offers the following additional guidance and examples to inform the content of these best practices.

Identity proofing—the process of verifying individuals' identities so that they can be issued credentials for access to a system such as a patient portal--is the foundation for identity management. Based on the results of the hearing, it is clear that in-person ID proofing provides the most protection. However, remote proofing is highly desired by some patient populations—such as, rural populations and the elderly-- and is needed to enable more patients to use patient portal accounts. Consequently, best practices for both options should be provided.

In-person identity proofing can be performed by the provider at the point of treatment, where a relationship and trust already exists. However, provider employees may not be familiar with the specifics of identity proofing and should be provided training on basics of this process. Providers may also rely on others to perform in-person identity proofing on their behalf, for example, notaries public.

Remote identity proofing should also be offered, but does raise more risks. Potential methods raised in the hearing include:

- Re-use of existing credentials. For example, witnesses at the hearing cited the use of credentials (user ID and password) already established for a Windows Live ID or Facebook account to establish/access a patient portal account.
- Third-party, knowledge-based authentication. This approach involves verifying identity by asking the patient questions (developed by a third-party vendor) based on information about them resident in public records. It should be noted that this approach will not work for all patient populations, such as minors for whom there is little or no public information available. Further, the approach is dependent on quality of the data available to the third party, and it may be expensive. Hearing participants also noted that patients may be unsettled if asked about non-health accounts—such as mortgage accounts—to create a portal account and thus, preparing patients in advance on the purpose of asking these questions is important. In addition, it is a best practice to use data not easily known to others, including family members.
- Verification against in-house systems. Provider entities may also verify identity using demographic matching against in-house practice management or other provider systems. As with knowledge-based authentication, a best practice is to use data not easily known to others, including family members.
- Use of technology. Providers could also use existing technology, such as personal computer cameras, to enable them to confirm the identity of the individual.

To further manage risks, remote ID proofing should be coupled with out-of-band confirmation, that is, using an independent, different channel of communication with the individual to confirm establishment of an account or other activity. Examples include (1) sending a letter to the patient using the home address on file, (2) sending an email to other known e-mail addresses for the patient, or (3) placing a confirming phone call to the patient.

Building on its previous recommendations on patient authentication, the Tiger Team believes that ONC should strongly encourage providers to use more than user ID and password (single factor authentication) to permit patient access to portals. In addition, ONC should strongly encourage providers, at least initially, to drive toward protections analogous to those used in online banking, especially given consumers' familiarity with these practices. The hearing results indicate that there are easily used second factors that would build on passwords and provide greater assurance. Examples include:

- additional knowledge-based questions posed to the patient,

- machine-to-machine technical controls that recognize the patient's customary device and trigger a request for additional authentication when a different device is used, and
- emails to known addresses, phone calls, and/or letters that request confirmation that patients actually accessed their account or notify them of unusual account activity.

The Tiger Team considered whether it should encourage the HITSC, though its Privacy and Security Work Group, to consider EHR certification standards in this area. However, given that hearing participants stressed that "one size does not fit all" and the need to take advantage of improvements offered by the evolving technology in this area, the Tiger Team concluded that certification standards may not be the best vehicle for accomplishing this. Instead, the Tiger Team recommended that best practices be disseminated to vendors.

The Tiger Team also considered whether it needed to make additional recommendations on the use of the DIRECT protocol when patients use the "transmit" function to authorize transmission of their information to a personal health record (PHR) or other third-party. The Tiger Team concluded that DIRECT is moving forward in way that is consistent with these recommendations. Specifically, when using the transmit function, the expectation is that the patient (or legal representative) will provide the DIRECT address to the provider to initiate the transaction. Patient control over this address should give providers a level of assurance that the information is being transmitted to the right person. As a result, the Tiger Team concluded that no further recommendations are needed at this time

The Tiger Team recognizes that although the problems with the use of passwords for authentication are well known, passwords are likely to continue to play a role in authentication for the foreseeable future. Thus, ONC should also disseminate, at a minimum, the very latest best practices in password management. In addition, technology options for authentication continue to evolve; ONC should continue to monitor and update policies as appropriate to reflect improved technological capabilities

Given the risks associated with credentialing patients for view/download/transmit and the critical importance of educating patients about the use of these functions, ONC should also disseminate best practices based on the previous HIT Policy Committee Recommendations regarding transparency of the risks and benefits of view/download/transmit to patients. (See attached transmittal letter.)

Finally, NSTIC, which would provide for credentials that could be re-used for a range of online purposes, should provide a more scalable solution for patient authentication in the future. ONC should continue to work with NIST to ensure that any issues unique to the health care environment are addressed in the development of the NSTIC approach.

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

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee