Privacy and Security Tiger Team

Trusted Identity of Patients in Cyberspace

Recommendations on Patient Identity Proofing and Authentication

January 8, 2012

Tiger Team Members

- **Deven McGraw, Chair**, Center for Democracy & Technology
- **Paul Egerman, Co-Chair**
- **Dixie Baker**, SAIC
- **Neil Calman**, Institute for Family Health
- **Carol Diamond**, Markle Foundation
- **Judy Faulkner**, Epic
- **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
- **Kitt Winter,** Social Security Administration

Recommendations (1) (DRAFT)

Overarching Recommendation: 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 EPs, EHs and CAHs sufficiently in advance of the onset of Stage 2 to enable planning.

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

Recommendation (2) (DRAFT)

- Recommendation 2: Such best practices should be consistent with the following overarching principles:
  - Protections should be commensurate with risks
  - Simplicity and ease of use for patients and consistent with "what they are willing to do"
  - Flexibility in methods offered—"one size does not fit all"
  - Leverage solutions in other sectors, such as banking
  - Accompanied by education that make these processes transparent to the patient
  - Build to scalable solutions (e.g., greater use of voluntary secure identity providers)
  - Solutions need to evolve over time as technology changes

Key Takeaways from Hearing (to help inform best practices) (DRAFT)

- ID Proofing
  - In person ID proofing provides the most protection.
  - However, remote proofing is highly desired by some patient populations (veterans, rural, elderly) & is needed to enable more patients to use these accounts.
  - Consequently, best practices for both options should be provided.

In-Person ID Proofing (DRAFT)

- Performed by provider where relationship/trust exists; training of provider employees on basics of identity proofing recommended.
- Provider may rely on others to perform in-person (for example, notaries public; may be more viable option post implementation of NSTIC)

Remote ID Proofing (1) (DRAFT)

- Remote ID proofing should be offered, but does raise more risks. Potential methods:
  - Rely on re-use of existing credentials (for example, credentialing for on-line sites like Facebook)
  - Third-party, knowledge-based
    - Dependent on quality of data, questions; may be expensive
    - May not address all patients, for example, minors <18
    - Patient education critical to address privacy concerns
  - In–house, demographic matching on practice management or other provider systems (Note that for knowledge-based or demographic data ID proofing solutions, best practice to use some data fields not known to others, including family members)
  - Use of technology (such as through computer cameras)

Remote ID Proofing (2) (DRAFT)

- To further manage risks, couple with out-of-band confirmation (using an independent/different channel to confirm identity) – for example, letter to confirm account establishment/access by right person; sending to other e-mail addresses; confirming phone call to patient; alerting of unusual activity in the account).

Authentication (1) (DRAFT)

- Previous 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
  - should also be mindful of guidelines for identification and not set requirements so high that patients are discouraged or cannot meaningfully participate

Authentication (2) (DRAFT)

- Post hearing: ONC should strongly encourage providers to use more than user ID and password (Level “2.5”), and at least initially, drive toward protections analogous to those used in online banking
- The Tiger Team considered whether it should encourage the HITSC, though the P&S WG, to consider certification standards in this area. However, given 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 approach at this time.

Authentication (3) (DRAFT)

- ONC should also disseminate, at a minimum, the latest best practices in password management
- Technology options for authentication continue to evolve; ONC should continue to monitor and update policies as appropriate to reflect improved technological capabilities.

Best Practices (draft) - Transparency

- 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 respond to previous Policy Committee Recommendations regarding transparency of risks/benefits of V/D/T to patients. (see backup slides)

Patient Use of DIRECT

- 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 PHR or other third-party.
- The Tiger Team concluded that DIRECT is moving forward in way that is consistent with these recommendations:
  - Specifically, the patient (or legal representative) provides the DIRECT address to the provider
  - No further recommendations are needed at this time
- Additional details on the use of DIRECT are shown on the following slide.

Future Solutions (DRAFT)

- 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

BACKUP SLIDES

Transparency Recommendations on View/Download (1 of 4)

- The Tiger Team opted to offer best practice guidance for providers (as well as vendors and software developers) participating in the Meaningful Use program as stated below. Such best practice guidance could be communicated by ONC through the Regional Extension Centers (RECs) as well as through the entities certifying EHR Technology.
  - Providers participating in the Meaningful Use program should offer patients clear and simple guidance regarding use of the view and download functionality in Stage 2.

Transparency Recommendations on View/Download (2 of 4)

- With respect to the download functionality, such guidance should be offered at the time the patient indicates a desire to download electronic health information and, at a minimum, address the following three items
  - Remind patients that they will be in control of the copy of their medical information that they have downloaded and should take steps to protect this information in the same way that they protect other types of sensitive information.
  - Include a link or links to resources with more information on such topics as the download process and how the patient can best protect information after download.
  - Obtain independent confirmation that the patient wants to complete the download transaction or transactions.

Transparency Recommendations on View/Download (3 of 4)

- With respect to the “view” functionality, such guidance should address the potential risks of viewing information on a public computer, or viewing sensitive information on a screen that may be visible to others, or failing to properly log out after viewing.
- Providers should also utilize techniques, if appropriate, that avoid or minimize the need for patients to receive repeat notices of the guidance on view and/or download risks.
- Providers should also request vendors and software developers to configure the view and download functionality in a way that no cache copies are retained after the view session is terminated. Providers should also request that their view and download functionality include the capability to automatically terminate the session after a period of inactivity.

Transparency Recommendations on View/Download (4 of 4)

- ONC should also provide the above guidance to vendors and software developers, such as through entities conducting EHR certification.
- Providers can review the Markle Foundation policy brief, and the guidance provided to patients as part of the MyHealtheVet Blue Button and Medicare Blue Button, for examples of guidance provided to patients using view and download capabilities.

United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

Overview of the Verification Requirements of the HIPAA Privacy and Security Rules

David S. Holtzman, JD, CIPP/G
Office for Civil Rights
Health Information Privacy Division

Privacy Rule Verification Standard

- The Privacy Rule (45 CFR 164.514 (h)) requires covered entities (CE) to verify the identity and authority of a person requesting protected health information (PHI), if not known to the CE.
- The Rule allows for verification in most instances in either oral or written form, although verification does require written documentation when such documentation is a condition of the disclosure.
- The Rule generally does not include specific or technical verification requirements to permit covered entities to fashion procedures that fit the size and complexity of their organization.
- The CE must also establish and document procedures for verification of identity and authority of personal representatives, if not known to the entity.

Implementing the Privacy Rule's Verification Standard

- For example, verification procedures that can be applied in an electronic health information environment:
- Consumers can agree with the CE to keep current their demographic information and personal representatives so the CE can appropriately authenticate each user of the network
- For persons claiming to be government officials, proof of government status may be provided by having a legitimate government e-mail extension (e.g., xxx.gov)
- Documentation requiring signatures may be provided as a scanned image of the signed documentation or as an electronic document with an electronic signature, to the extent the electronic signature is valid under applicable law.

Security Rule Verification Standards

- The Security Rule layers additional safeguards for the verification of identity when attempting to access electronic protected health information (e-PHI).
- The information access management standard (45 CFR 164.308(a)(4)(i)) requires a covered entity or their business associate to have formal, documented policies and procedures implemented for the authorization of access to e-PHI that are complimentary with those of the Privacy Rule.
- The person or entity authentication standard (45 CFR 164.312(d)) requires a covered entity to implement procedures or security measures to verify that a person or entity seeking access to e-PHI is the one claimed.