HIT Standards Committee

Hearing on Trusted Identity of Patients in Cyberspace

November 29, 2012

Jointly sponsored by HITPC Privacy and Security Tiger Team and HITSC Privacy and Security Workgroup

Dixie Baker, P&S Workgroup Chair

December 19, 2012

Hearing Focus

Stage 2 meaningful use takes a significant step forward in empowering patients to play an active role as part of their own health care team. Specifically, Stage 2 incorporates the HITECH provisions for patients to be able to view, download, and forward to a third party an electronic copy of their health information. Thus for Stage 2, identity proofing and authentication of consumers become very, very important.

- Identity Proofing of Consumers
- Authentication of Consumers

Definition: Identity Proofing

- Identity Proofing is the process of collecting and verifying information about a person for the purpose of proving that a person who has requested an account, a credential, or other special privilege is indeed who he or she claims to be
  - May include, for example, driver license, passport, birth certificate
  - Identity proofing is performed before the account is created (e.g., portal, email), the credential is issued (e.g., digital certificate) or the special privilege is granted

Definition: Authentication

- Authentication is the process of establishing confidence that an individual who uses a credential that is known to the system (e.g., login name, digital certificate) is indeed the person to whom the credential was issued
  - Three types of authenticators:
    - Something you know (e.g., password)
    - Something you have (e.g., smartcard, hard token, mobile phone)
    - Something you are (e.g., fingerprint)
  - Multi-factor authentication requires more than one type
  - Authentication is performed each time a user logs into an account (e.g., portal, email) or otherwise uses a credential

Purposes of Hearing

- Aiming toward “best practices” for meaningful-use Stage 2 and forward-looking practices for Stage 3
- Recommendations
  - Principles
  - Best practices
  - Transmit functions for consumer communications
- Privacy and Security Tiger Team will present policy recommendations to HIT Policy Committee in January

Hearing Agenda

- Introductions from TT/WG Chairs and ONC
- HIPAA Privacy and Security Rule Requirements for Verification of Identity (David Holtzman, HHS Office for Civil Rights)*
- Panel One: Why identity proofing and authentication of patients are important and what are the key issues.
- Panel Two: What patient identity proofing and authentication methods are in use now.
- Panel Three: What identity proofing and authentication solutions are on the horizon.

*ONC summary of relevant HIPAA requirements included in Appendix

Principles Gleaned from Hearing

- Want ID proofing and authentication to be protective and easy to use
- Need flexible solutions
- Patients need to be educated on risks and protection that ID proofing and authentication give them
- Want patients to be able to have an identity that can be used by multiple providers
- Solutions need to evolve over time

Identity Proofing Methods

- In person
  - Performed by provider where relationship/trust exists; training of provider employees on basics of identity proofing needed
  - Some use methods that rely on third parties (such as notaries public)
- Remote
  - Reuse of existing credentials
  - 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
  - Demographic matching on practice management or other provider systems
  - Should be accompanied by out-of-band confirmation (e.g., letter)
- Need to share “best practices”

Authentication Methods

- Tiger Team/HITPC previously recommended a minimum of user name and password
- Questioned whether a higher level of assurance was needed
  - No single level of assurance is right for all purposes
  - Need “best practices” that move in the same direction as online banking
  - Need transparency regarding risks and benefits for download and transmit
- Need to move toward National Strategy for Trusted Identities in Cyberspace (NSTIC) approach

Privacy and Security Workgroup Observations

Deven McGraw (Chair Privacy and Security Tiger Team) met with Workgroup to discuss hearing. These are some of the observations gleaned from that discussion.

- Capitalize on banking industry guidelines
- Define level of assurance required, not how to be accomplished
- Should not attempt to align provider and consumer methods for ID proofing and authentication – need higher level of assurance for providers than for patients
- Best to establish best practices for ID proofing and standard for authentication

Transmitting to Consumers and Third Parties

- 2014 Edition of Standards and Certification Criteria require capability to use Direct to transmit health information to patients and third parties
  - CMS has made clear that transmission using transport standards other than Direct (SMTP, FTP, REST, SOAP, etc.) will still count toward the patient-action (5%) measure
- HIT Policy Committee has raised questions regarding the use of Direct for transmissions to consumers, given perceived complexities associated with the issuance, use, and management of digital certificates
  - Anticipate that PHR service providers will provide Direct addresses, and associated digital certificates, to consumers
  - As a measure of identity proofing, providers will need to obtain Direct address directly from patient requesting record transmission

Next Step

- Privacy and Security Tiger Team will present findings and recommendations on identity proofing and authentication to HIT Policy Committee in January

Appendix: OCR Summary of Relevant HIPAA Requirements

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.