Patient Portal
Identity Proofing & Authentication
Guidance from the HIMSS Identity Management Task Force
May 2016
Identity Management Task Force

• Represents HIMSS membership with regard to national and industry initiatives on identity management, such as the National Strategy for Trusted Identities in Cyberspace Identity Ecosystem Steering Group (NSTIC IDESG) and other national policy and technical efforts.

• Develop tools and resources that will assist HIMSS members on identity management issues.

• Membership is open to all HIMSS members
Key Identity Management Task Force (IDM TF) Recommendation - 2015

All mechanisms or processes that provide electronic access by patients to their own protected health information (PHI, as defined by HIPAA) must be capable of employing user identity proofing and authentication at a high level of confidence, greater than or equal to National Institute of Standards and Technology (NIST) Level Of Assurance (LOA) 3 or equivalent (as determined by a documented HIPAA risk analysis).
Patient Proofing and Authentication Today:

**Proofing**
Process for initial/periodic verification before issuing credentials.

1. At healthcare office visit patient given one time code.
2. Patient later uses to activate on-line account.
3. Some use Knowledge Based Authentication (KBA) for remote proofing.

**Authentication**
Credential patient uses for on-line access

1. UserID and password!
2. UserID and password!!
3. UserID and password!!!
Patient Portal Proofing and Authentication
Today: Broken in Many Ways

• Attacks against healthcare are growing
  – proofing and authentication techniques are 20 years old
• Attackers spent 20 years honing skills against financial services
  – healthcare is easy pickings for them
• Healthcare has to deal with proxy and anonymous access use cases
  – proxy access insecure with unauditable password sharing
• HOWEVER,
  – A large proportion of the patient population now has access to smartphones, and newer techniques for proofing and authentication allow us to raise the security bar while lowering costs and improving usability.
We begin with NIST 800-63-2

• U.S. Federal Government NIST SP 800-63-2 specification provides excellent starting point for our guidance.

• We also take into account and anticipate the emerging work on 800-63-3.

• Current NIST specification has four “Levels Of Assurance” or LOAs for identity proofing and authentication.

• We aim for a level of high confidence in identity, equivalent to NIST LOA-3, but tailor our guidance to specific needs of healthcare.

All security is a trade off between level of assurance, ease of use and total cost of ownership.

We strive for a balance that is sensible for healthcare.
We discuss three distinct use cases

1. The general use case which applies to most patients most of the time.

2. The proxy use case where access is delegated. For instance a parent accessing a child’s account, or a care-giver for an elderly patient.

3. The anonymous use case where the clinic relying on the credential can trust the digital identity is valid, without actually knowing the actual identity of the user.
Proofing Recommendation Summary

- Patient provides: government issued Photo-ID, a health insurance card, a smartphone/cellphone number and an email address.

- Organization compares photo/insurance-card to actual user and cross references personal information.

- They should actively ensure that the user is in possession of phone and email address provided.

- Video call can be used to emulate in-person proofing remotely with the same requirements. KBA alone does not suffice today and must be supplemented by other techniques.

- Simple proxy mechanisms must be incorporated into patient portals for improved convenience while maintaining security; credential sharing is not acceptable.

- Pseudonyms should be assigned to fully identity proof individuals when needed for anonymity.

- In all cases the organization should maintain an event log capable of reconstructing the proofing process.
Applying Risk Analysis to Proofing

• Forgeries of Photo-IDs will remain a threat vector. Strategy to mitigate this risk is to also require validation of email and phone number. The difficulty in forging all three raises the bar sufficiently for now.

• A recent NIST paper points out variety of technical, policy and implementation considerations for determining the strength of identity proofing. NIST suggests consideration of each component function, such as: identity resolution; identity validation; identity verification, and activity history.

Authentication

• To access PHI online, we require two-factor authentication, specifically including a “something you have” factor. In practice this is the user’s smartphone typically with the ability to generate or receive one time codes or passwords via text or using some other secure authentication process.

• As smartphone biometrics and standards like FIDO mature, this will effectively provide a path to incorporating biometrics in the future.

• Authentication techniques for proxy delegates or anonymous patients must not be different from those used for the patients themselves. The strength of authentication for proxy access must be at least as strong as for the original user.

• The organization should maintain a log of all authentication events whether they were successful or not.
Applying Risk Analysis to Authentication

- Threats against authentication include theft, duplication, discovery, eavesdropping, off-line cracking, phishing and social engineering. Any proposed solution must be analyzed along all these fronts in a risk analysis.

- Incorporating a smartphone significantly raises the bar and such a multifactor implementation can be rationalized with a risk analysis to provide a high confidence authentication of identity.

- Recent NIST paper says that analysis of potential vulnerabilities across the stages of presentation, capture, enrollment, comparison, and decision could be the basis for calculating the strength of biometric authentication

Addressing Proxy Access

- Patient portals must establish a system of proxy access for improved usability and convenience while maintaining appropriate security.
- Proxy mechanisms may be simple “all-or-none” types at first and then can evolve to provide better and more automated services to users as policies and techniques improve.
- Identity proofing of proxy delegates can use the informed authorization of the patient if the usual identity proofing process is impractical.
- Authentication techniques for PHI access by proxy delegates must not be different from those used for the patients themselves.
- The strength of authentication for proxy access must be at least as strong as for the original user.
Addressing Anonymous Access

• In a typical healthcare environment, all patients must be uniquely identified in some way so that the permanent records of their care are not confused with the care records of other patients.

• Patients should be proofed at a high level of confidence.

• Patients have a right to request anonymity to add a layer of privacy protection to their records. We recommend they be assigned a pseudonym.
Conclusion and Next Steps

• Incorporation of smartphones as a second factor into the processes of identity proofing and authentication will significantly improve the security of electronic interactions with many patients while minimizing the additional cost and difficulty.

• In other verticals such as financial services, proofing and authentication (front door locks) have been augmented with back end risk management (motion detector alarms). We expect the same to happen in healthcare and will augment our guidance in the future.

• Read the full identity proofing and authentication guidance document:
  
Appendix

Supplemental Information
Consistent with ONC’s Shared Nationwide Interoperability Roadmap

Supports the Precision Medicine Initiative

Research cohort that will engage a million or more Americans who volunteer to contribute their health data over many years to improve health outcomes, fuel the development of new treatments for disease, and catalyze a new era of data-based and more precise preventive care and medical treatment.

Data Security Policy Principles and Framework

Access Control

Identity Proofing - PMI organizations should develop a policy for verifying the identity of users and contributors (e.g., participants and healthcare provider organizations), prior to granting credentials for access to or contribution of PMI data.

Credentials - PMI organizations should use innovative approaches for authentication so that over time they do not rely on username and password alone, and should use strong multi-factor authentication for users of PMI data.

Authentication - Risk-based authentication controls should flow from the organization’s security risk assessment, and should be commensurate with the type of data, level of sensitivity of the information, and user type.