

Introduction:

The following recommendations were developed by the Confidentiality, Privacy and Security workgroup (CPS workgroup) on the topics of identity proofing and user authentication as they relate to three near-term breakthrough areas defined by the American Health Information Community (AHIC):

- Secure messaging between patients and clinicians to enhance care delivery to the patient;
- Providing secure access to historical laboratory results stored within electronic health records (EHRs); and
- Providing secure access to patient registration summary and medication history information stored within personal health records (PHRs).

The recommendations provided below have been categorized as follows:

- General Recommendations – These are recommendations that apply across all three near-term breakthrough areas: secure messaging, EHRs, and PHRs; and
- Breakthrough Recommendations – These are recommendations that apply to a particular near-term breakthrough area.

For each recommendation, additional information is provided in the form of options, assumptions, constraints, scope (to clarify and/or qualify a recommendation) and [*guidance (TBD)*].

- Options are used when the interpretation of a recommendation may differ across environments;
- Assumptions are used establish any necessary pre-existing conditions;
- Constraints are identified if there are other activities that need to be/or are currently in the process of being completed and the recommendation depends on those processes to advance the issue;
- Scope is used to describe the specific area of impact for a recommendation (e.g., the environment, application, or service) and;
- Guidance (TBD)

These recommendations are not intended to represent a comprehensive or complete set of recommendations for identity proofing and user authentication for the healthcare industry. They are recommendations developed based several workgroup discussions and the public hearing testimony provided to the CPS workgroup on September 29, 2006. Furthermore, it is not the intent of the workgroup to issue recommendations that introduce barriers to the provision of efficient and effective healthcare to patients. Where a recommendation may be very suitable for a large operating environment such as a hospital or insurer, it may not for a small provider, and vice-versa. To that end, the following general assumptions have been made with respect to all of the recommendations.

General Assumptions:

- 1) *At a minimum, these recommendations advance the specific charges of the Chronic Care, Electronic Health Record (EHR), and Consumer Empowerment workgroups, and, where possible should attempt to meet aspects of the each of the workgroup's broad charge.*
- 2) Information exchanged during secure messaging or accessed in an Electronic Health Record (EHR) or Personal Health Record (PHR) will be of clinical relevance, and will be personal and potentially sensitive.
- 3) User **authentication** is separate and distinct from user **authorization**. **Authentication** is the reliable identification of a user – proof that someone is who they claim to be,, whereas **authorization** is the issuance of credentials to an authenticated user allowing access to the clinical messaging tool, the EHR, or the PHR, as the case may be. User **authorization** requires an understanding of the user's roles and privileges before determining if access to a resource should be granted. The two security functions are complementary, yet very distinct, and the recommendations below only address issues related to **authentication**.
- 4) When defining identity proofing and user authentication procedures, it is important to understand that they are a part of the overall process for issuing electronic identity credentials. If they are not of equal level, the overall strength of the electronic identity credential may not satisfy the requirements of the application/service.
- 5) The implementation of peer to peer secure email is challenging and introduces many security issues, and is generally not recommended for the exchange of sensitive healthcare information.

General Draft Recommendation(s):

GR-1: The general policy recommendations of this work group are not a substitute for a well implemented, onsite risk assessment. A thorough risk assessment is generally considered to be a best practice in information security.

Options:

-

Assumptions:

- All healthcare data is sensitive

Constraints & Applicable Info:

-

Scope:

-

GR-2: Given that the healthcare community is comprised of many affiliated organizations, with personnel operating in many different roles, the establishment of a

consistent identity trust model is necessary. The WG recommends that further work be performed on federated identity architectures and trust establishment procedures.

Options:

-

Assumptions:

-

Constraints & Applicable Info:

-

Scope:

-

GR-3: User authentication for networked health services, should be implemented through the use of a two-factor electronic authentication (e.g. digital certificate or biometric, and password), or through the use of single-factor authentication (e.g., username and password) where the patient decides to assume the risk presented by single-factor credentials.

Options:

- Different combinations of identification and proofing may apply to those accessing electronic health information (e.g., provider, patient, third-party).
- Patients may benefit from the option to employ additional privacy features to ensure greater levels of confidentiality when needed (e.g., an option to apply a third factor of identification).

Assumptions:

- In order to use single-factor authentication, the patient should be educated about the risks associated with choosing to participate in such a service.

Constraints & Applicable Info:

-

Scope:

- This recommendation applies to all three breakthroughs.

Secure Messaging Focused Draft Recommendation(s):

SM-1: Clinicians or other entities who offer secure messaging services should implement some form of in-person patient identity proofing procedures for patients. In some circumstances, such as having existing patients that have a long history with a clinician, this may be accomplished by the use of historical data and practice knowledge. This would allow patients well known to the practice to begin using secure messaging to communicate with the practice even if their next scheduled in-person visit will not take place for some time.

Options:

-

Assumptions:

CPS WORKGROUP DOCUMENT
*****Working Draft ***Pre-decisional*****

- The clinician and the patient have the requisite clinician patient relationship as governed by medical ethics and applicable law.
- The patient and clinician both should authorize the use of secure messaging between them before it commences. This does not substitute for patient education, outreach, and other activities designed to inform the patient about secure messaging.
- When secure messaging is not directly provided by a clinician, clinicians should be initially identity proofed at the sponsoring organization.

Constraints & Applicable Info:

- DoD conceptual secure messaging systems may provide useful insight into this discussion.
- Performing in-person identity proofing separately for secure messaging is difficult to scale, and may thus be best accomplished via widely accepted identity proofing solutions.

Scope:

- This recommendation only pertains to secure messaging and may not apply or scale to various electronic health environments and services.
- Acknowledge that some testimony confirmed that secure messaging accounts allows patients to also access PHR/EHRs.

SM-2: <<Place Holder>> There were specific questions about how identity proofing is currently being done (e.g. a scoring mechanism for certain types of documents or information) and what types of documents are commonly being used in the clinical environment or other industries. More information is required/is currently being collected on the processes involved in identity proofing.

Options:

- CPS Workgroup should review and consider best practices and standards from a variety of industries, beyond healthcare and financial services, to ensure recommending the most effective guidelines.
- CPS Workgroup should consider the lifecycle of technologies discussed to ensure that recommendations remain relevant for a reasonable duration.
- CPS Workgroup could refer this issue to HITSP or consult another appropriate authority.

Assumptions:

-

Constraints & Applicable Info:

-

Scope:

SM-3: At the request of the patient, two steps should be performed in order to grant any proxy (authorized patient representative) the ability to secure message with a clinician on their behalf. Step 1, the proxy should be identity proofed in some way either by the clinician or a trusted third party, and Step 2, the clinician should verify that proxy has the authority to act on behalf of the patient.

Options:

- In-person Proofing – To reduce risk and provide clinicians with a higher level of assurance that a proxy is who they say they are, clinicians have the option to, and should perform, in-person identity proofing for any proxy the patient requests to secure message with the clinician on their behalf. As discussed in SM-1, clinicians should be able to rely on existing (long standing) proxy relationships as their method way to determine the issuance of secure messaging credentials.
- Trusted Third Party – While in-person identity proofing is considered a current best practice, clinicians may use other methods of identity proofing such as those attested to by a trusted third party (e.g. notarized documents containing identity verification information).
- Override mechanisms should be considered to facilitate care during emergency situations where the patient lacks capacity to grant access to new users of patient information.

Assumptions:

- State law will determine the documentation needed to authorize a proxy to participate in secure messaging on behalf of the patient. This would not preclude a patient from sharing a secure message that the patient received with a caretaker.
- Rules will be developed for minors consistent with applicable state law(s).

Constraints & Applicable Info:

-

Scope:

- This recommendation only pertains to secure messaging and may not apply or scale to various electronic health environments and services.
- Acknowledge that some testimony confirmed that secure messaging accounts allows patients to also access PHR/EHRs.

SM-4: Clinicians should use an interface such as a secure (encrypted and mutually authenticated) web-portal to support secure messaging with their patients. The clinician should also educate the patient on the proper usage of the secure web-portal, to ensure that both parties understand how communication will take place and with whom (clinician or delegated person).

Options:

-

Assumptions:

-

Constraints & Applicable Info:

- Education and support for both patients and data users will need to be considered specific to use and sharing of information and to HIPAA requirements.

Scope:

-

PHR Focused Draft Recommendation(s):

PHR-1: <Requires more workgroup discussion>

Options:

- The use of knowledge-based online identity proofing solutions (e.g. verifying phone number information with caller ID).
- In person identity proofing at the sponsoring organization or a trusted third party.

Assumptions:

- PHRs by nature are meant to be readily available, accessible, and portable.

Constraints & Applicable Info:

- Data agreements and relationships between knowledge providers and PHR service providers would need to be effectively established

Scope:

-

EHR Focused Draft Recommendation(s):

EHR-1: The source document(s) used to perform identity proofing should be securely stored and maintained separately from the patients' EHR or other clinical data.

Options:

-

Assumptions:

-

Constraints & Applicable Info:

- The intent of this recommendation is to limit data breaches and prevent [medical] identity theft.

Scope:

-

EHR-2: Simply converting from a paper-based practice to one with EHRs should not require a clinician to identity proof their patients. However, if the converted EHR system provides patients with the ability to access their own EHR via the Internet, clinicians should follow the identity proofing recommendation schema noted above in SM-1.

Options:

-

Assumptions:

-

CPS WORKGROUP DOCUMENT
*****Working Draft ***Pre-decisional*****

Constraints & Applicable Info:

- During the conversion from paper to electronic records, issues often arise including new capabilities for patients, such as electronic access to view their EHR.
- CPS may wish to consider options whereby providers begin entering data into systems regardless of the actual use of EHR and PHR simply to begin the process of gathering data in electronic format to facilitate adoption when systems are implemented. Population of data might begin as early as 2009 to allow for sufficient document health information to render the EHR useful.

Scope:

-