

DRAFT: Identification and Authentication Recommendations

I. Patient Access to Information in a Provider's EHR (such as via a portal or tethered/shared PHR)

A. Identity: The HIPAA Security Rule already places obligations on covered entities to implement policies and procedures for granting access to ePHI.

Questions that covered entities must address include:

- Who should perform identity proofing;
- What method is used (such as in-person or remotely, or bootstrapping on identity performed by a trusted third party);
- What is acceptable identification documentation; and
- Does the documentation need to be verified.

Recommendation:

1. The Tiger Team supports entities making these determinations based on their own assessments of what is necessary to address the risks of inappropriate access. However, we recommend such assessments be guided by the following principles:

- a. Providers must manage the risk of inappropriate access; however, they should not set the identification requirements in a way that discourages or inhibits patients from participating.
- b. Providers should offer the option of “registering” for access during an office or facility visit – but they should also offer options in addition in person-identification. Permitting only in-person identification may make participation difficult for individuals who live in rural areas, or who lack reliable transportation or who face health, financial or other barriers to coming into the office or facility.
- c. One technique for remote identification is requiring the individual to provide information that is known to both parties. Providers using such a method should be careful to choose information beyond basic demographic information (such as address, date of birth, social security number) that might be known or knowable by an unauthorized person.
- d. Providers should require more stringent proof of identity for access to patient identifiable data in the EHR. Information required to access other electronic services (such as signing up for an appointment or indicating interest in a portal or PHR that is merely designed to trigger follow-up) may not need stringent identity.
- e. Providers should also consider the populations they serve in setting identification requirements (for example, providers should consider primary languages spoken, likelihood of possessing photo or government-issued identification, etc.).
- f. Providers should consider consulting their patients (such as if they have a patient advisory group) to get feedback on what will work

best for them while also providing appropriate security (VA has done this with MyHealthVet).

2. **ONC [HHS?] should [work with NIST to?] provide guidance to providers on trusted identification methods. Such guidance should be updated to reflect federal government e-identification efforts (such as the National Strategy for Trusted Identity in Cyberspace).**

B. Authentication

Recommendations:

1. **Providers should require at least a user name and password to authenticate patients.**
 - a. **This single-factor authentication should be a minimum – providers may want to at least be able to offer their patients additional security (such as through additional authentication factors) or provide such additional security for particularly sensitive data.**
 - b. **In setting authentication requirements, providers should also be mindful of guidelines for identification and not set requirements so high that patients are discouraged from participating or cannot meaningfully participate (for example, by requiring complicated passwords).**
2. **Certified EHRs should include a capability to detect and block programmatic attacks or attacks from a known but unauthorized person (such as auto log-off after a certain number of unsuccessful log-in attempts). Having this capability in the EHRs provides providers with options for deploying technology-supported password management programs.**
3. **[same recommendation as for identity] ONC [HHS?] should [work with NIST to?] provide guidance to providers on trusted authentication methods. Such guidance should be updated to reflect federal government e-identification efforts (such as the National Strategy for Trusted Identity in Cyberspace).**

II. Recommendations for Authentication of Individual Users of a Certified EHR

The Tiger Team had previously issued recommendations on authentication of entities using EHRs to exchange electronic health information. Our recommendations requiring entities to obtain digital certificates, and recommending that ONC establish a process for accrediting digital certificate issuers, were adopted by the Policy Committee on [fill in date].

With respect to individual users of EHRs, the HIPAA Security Rule requires covered entities to protect against any reasonably anticipated uses or disclosures not permitted or required by the HIPAA Privacy Rule. The Security Rule also requires covered entities to implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. However, the Security Rule does not specify authentication options, assurance levels or verification requirements.

As a result, the Tiger Team is looking to establish some stronger authentication policy as part of governance for the Nationwide Health Information Network (NwHIN).

Recommendations:

- 1. Organizations that are seeking to exchange information as part of the NwHIN should be required to adopt *baseline* user authentication policies that require more than just user name and password for remote access. At least two factors should be required. Remote access is defined as access over a public network like the Internet.**

-The Team was not comfortable with requiring the application of the NIST or DEA requirements for all authentication because of the stringency of the second factor requirement.

-The Tiger Team was particularly concerned about remote access (vs. access within the physical structure of an entity), but we had a difficult time initially setting parameters for what constitutes "remote" access. Does the definition above get it right? Do we need to specifically exempt access using a VPN?

-Should the Standards Committee be asked to determine which are appropriate factors for two-factor authentication?

- 2. These recommendations are intended to set a baseline for user authentication; organizations and entities can adopt more stringent requirements.**
- 3. For more sensitive, higher risk transactions, an additional authentication of greater strength subsequent to an initial authentication may be required, as has already been recognized with the DEA policy covering prescribing controlled substances. Additional work may be needed by the Policy Committee and ONC to identify the potential use cases that might require authentication above the baseline requirement.**
- 4. NwHIN Policies should be re-assessed for consistency with other national identity efforts, technology developments, such as National Strategy for Trusted Identity in Cyberspace.**

5. **ONC should also work to develop and disseminate evidence about the effectiveness of various methods for authentication and reassess NwHIN policies accordingly.**
6. **For writing e-prescriptions for controlled substances, Certified EHRs should have capability for the two-factor authentication, at a minimum consistent with DEA rule.**