

Privacy and Security Tiger Team Recommendations

Over the last several months, the Tiger Team has been evaluating a set of topics to ensure that security protections are in place to achieve public trust in health IT and health information exchange. This document outlines specific recommendations for the following:

- I. Authentication of Individual Users (Providers) of Certified EHR Systems**
- II. Patient Access to Information in EHR Systems, including Identity Proofing and Authentication of Patients**
- III. Additional Privacy and Security Policy Recommendations to Support Stage 2 Meaningful Use Objectives or EHR Certification Requirements**

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

The Tiger Team had previously issued recommendations on authentication of organizational 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 November 19, 2010.

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).

A. Policy 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 EHR user authentication because of the stringency of the second factor requirement.

- The Tiger Team was particularly concerned about remote access (vs. access within an entity’s private network), but we had a difficult time initially setting parameters for what constitutes “remote” access. We offer the definition above as a starting point, but through the rulemaking process ONC should seek comments both on what constitutes remote access, as well as the impact of two-factor authentication on providers. For example, Tiger Team members raised questions about whether two-factor is achievable via hand-held devices and whether requiring two-factor could result in providers having to carry multiple tokens for all of the organizations/institutions where they practice.
 - The Standards Committee also should provide recommendations on 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. Such policies should also be re-assessed to address innovations in technology both within and outside of the healthcare sector.**
 - 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.**

B. Stage 2 Meaningful Use

At the request of ONC, the Tiger Team identified additional Privacy and Security components that are (1) related to currently proposed Meaningful Use Stage 2

Objectives, and (2) require EHR functionality and/or technical standards to be required in certification for stage 2.

Related Meaningful Use Objectives: e-prescribing, exchange of laboratory data, connecting to external providers or an HIE, sending care summaries to other providers

- 1. Eligible Providers and Eligible Hospitals should be required to obtain digital certificates per the Tiger Team’s previous recommendations.**
 - 1a. The EHR certification process should include testing on the use of digital certificates for appropriate transactions.**
- 2. Eligible Providers are required to comply with the DEA rule regarding e-prescribing of controlled substances.**
 - 2a. For e-prescribing of controlled substances, stage 2 certification testing criteria for EHRs should include testing of compliance with the DEA authentication rule, which requires two-factor authentication.**

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

The HIPAA Security Rule already places obligations on covered entities to implement policies and procedures for granting access to electronic personal health information (ePHI), including requiring covered entities to implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. However, the HIPAA Security Rule does *not* specify authentication options, assurance levels or verification requirements.

A. Identity Proofing: In order to ensure that person seeking access is the one claimed, it is essential that identity proofing occur. 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.

Policy Recommendations:

- 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 to get feedback on what will work best for them while also providing appropriate security (VA has done this with MyHealthVet).
- 2. ONC 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) and innovations in technology (both within and outside of the healthcare sector).**

B. Authentication

Policy 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. ONC 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) and innovations in technology (both within and outside of the healthcare sector).**

C. Stage 2 Meaningful Use

- 1. Certified EHRs should include a capability to detect and block programmatic attacks or attacks from a known but unauthorized person (such as auto lock-out 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.**
- 2. Eligible Providers and Hospitals should deploy audit trails for a patient's portal, and at least be able to provide these to patients upon request. Audit trail capability for the portal will need to be part of Stage 2 certification requirements.**
- 3. Patient portals also should include appropriate provisions for data provenance, which is accessible to the user, both with respect to access and also upon download.**
 - o Further discussion will be needed to flesh out the details (for example, what information is needed to be included in provenance both for access to information in a portal and that is included with**

the information upon download; balancing accessibility with user interface issues; etc.).

4. **Patient portals should include mechanisms that ensure information in the portal can be securely downloaded to a third party authorized by the patients.**

III. Additional Privacy and Security Policy Recommendations to Support Stage 2 Meaningful Use Objectives or EHR Certification Requirements

A. Policies to Promote EHR Security – Security Risk Assessment

Relevant Meaningful Use Objective: conduct or review a security risk assessment and implement security updates.

1. **In Stage 1 of Meaningful Use, Eligible Providers and Eligible Hospitals are required to conduct or review a security risk analysis in accordance with the HIPAA Security Rule and implement security updates as necessary and correct identified security deficiencies as part of the risk management process. The Tiger Team recommends that this measure also be included in Stage 2 of Meaningful Use.**

We have an additional recommendation with respect to the risk assessment required for stage 2 of meaningful use – and below we provide background and the rationale for the recommendation.

2. **For Stage 2 of meaningful use, providers and hospitals must address encryption/security functionalities for data at rest, which includes data located in datacenters and also data in mobile devices (e.g. laptops, PDAs, etc). Providers and hospitals must attest that they have done this as part of their required security risk assessment.**

Rationale:

All participants in the meaningful use program are required to comply with the HIPAA Privacy and Security Rules. The HIPAA Security Rule requires that covered entities managing electronic protected health information (or “E PHI”) implement administrative, technical and physical safeguards to protect ePHI. The Security Rule sets forth a number of implementation specifications for complying with the Rule, some of which are required; but a number of these specifications are “addressable” to give covered entities some flexibility. If a specification is “addressable,” the covered entity must implement it unless the entity determines that it is not reasonable and appropriate to do so. In such a case, they must implement an equivalent alternative if a reasonable and appropriate one exists. The covered entity is required to document this decision. A number of the security

functionalities of certified EHRs provide support for addressable implementation specifications; encryption of data at rest is one of them.

The HHS Office of Civil Rights (OCR) is responsible for interpreting and enforcing the HIPAA Security Rule. Adam Greene of OCR has talked recently about the role that certified EHRs play in determining HIPAA security rule compliance. At the 2011 HIMSS Annual Meeting, Adam stated that “an entity (either an eligible professional or hospital) that manages a certified EHR system that has built-in technical safeguards for the confidentiality, availability or integrity of ePHI *will be expected under the HIPAA Security Rule to have those system safeguards (e.g., encryption) in operation.*” This is not issued as formal OCR Guidance and is not the same as stating that encryption is required by the Security Rule, as an example – but it does mean that eligible providers and hospitals could have a harder time convincing regulators that it was reasonable for them not to implement it.

The Tiger Team discussed a range of potential recommendations regarding the Security Rule’s “addressable” implementation specifications – specifically those supported by certified EHR security functionalities. We considered whether there were particular HIPAA security compliance issues that were problematic to building and maintaining public trust in health IT and electronic health information exchange.

Since the implementation of the new federal breach notification rules for HIPAA-covered entities, covered entities have been required to promptly report to HHS breaches of unencrypted PHI that affect more than 500 individuals. The overwhelming number of these breaches has been caused by thefts or losses of unencrypted data at rest (theft of laptops and workstations, loss of removable media, etc.). Of the 221 breaches involving more than 500 affected individuals reported to HHS by December 31, 2010, 51 percent were due to theft (e.g. laptops and smartphones). Another 21 percent of breaches were the result of unauthorized access or disclosure of protected health information, 15 percent were because of loss, 7 percent from hacking or other IT incidents, and 6 percent from improper disposal. “A little less known fact” is that there have been more than 14,000 breach reports involving less than 500 affected individuals.¹ In each case, had the data subject to theft or loss been encrypted, there would have been no breach or risk to individual health information to report to regulators.

Some have called the list of entities experiencing a breach or data loss of this magnitude “the wall of shame.” However, the impact of these breach reports goes beyond the individual institutions and organizations involved. This is a serious issue that the Tiger Team believes will negatively impact

¹ http://www.cardiovascularbusiness.com/index.php?option=com_articles&article=26447

public trust in EHRs if it is not more effectively addressed. Consequently, we believe HHS should use the meaningful use criteria to help shine a spotlight on this persistent problem. The Team recognizes that covered entities may reasonably use different approaches for protecting data at rest depending on the location, portability and immediate use of the data. For example, data at rest on portable devices and media (such as laptop computers and USB “thumb drives”), data on backup media (such as backup tapes), data stored as “hot” backups (on disk drives located at a remote data center) and data residing in an active operational database for an Electronic Health Record system need to be evaluated separately due to the differences in the ability secure the data, the likelihood that the data could be breached and the operational impact of encrypting the data. If data center disk drives are not encrypted, then appropriate security policies need to be established to ensure that such disk drives are properly disposed. The recommendation below does not ask for covered entities to do any more than what the Security Rule already requires them to do with respect to any addressable implementation specification – but the Team believes that highlighting compliance with the “encryption of data at rest” addressable implementation specification provides additional policy support for tackling this persistent problem.

B. Policies to Promote Accurate Patient Matching

Related Meaningful Use Objective: using an EHR to electronically record, modify, and retrieve patient demographic data
--

- 1. Eligible Providers and hospitals are required as part of Stage 1 of Meaningful Use to enter patient demographic data, and Stage 1 certified EHRs must enable a user to electronically record, modify, and retrieve patient demographic data. The following Tiger Team Recommendations relevant to accurate patient matching (and adopted by the Policy Committee) should apply to certification of EHRs for Stage 2:**
 - a. HIT Standards Committee should identify standard formats for data fields that are commonly used for matching patients (for example, name, DOB, zip, address, and gender).**
 - b. HIT Standards Committee should specify standards that describe how missing demographic data should be represented during exchange.**
 - c. The Tiger Team heard testimony that USPS normalization of addresses would be beneficial to the patient matching process, but the Tiger Team did not want to make a recommendation at that detailed a level. As a result, the HIT Standards Committee is**

requested to consider whether USPS address validation and normalization would be beneficial to improved matching accuracy and whether it should be added to the demographic standards.

- d. Stage 2 certification criteria should include testing that (i) appropriate transactions are sent/received with the correct demographic data formats and (ii) data entry sequences exist to reject incorrectly entered values.**