

Policies to Promote EHR Security

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

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.

1. The Tiger Team recommends that this measure also be included in Stage 2 of Meaningful Use.

On our last call, we began a discussion of whether to use the meaningful use policy lever to encourage eligible providers and hospitals to do more on security, particularly with respect to those provisions of the HIPAA Security Rule that are addressable and not per se required. We discussed “shining a spotlight” on the need for providers to address encryption at rest (determine when they are implementing it, and if not, what other measures they are taking to protect data) by specifically requiring eligible providers and hospitals to specifically address how they are implementing encryption at rest, which is an addressable provision under the Security Rule. Draft language for that option 2A:

2A. The Tiger Team recommends that providers and hospitals be required to specifically address how they are implementing the certified EHR encryption functionalities for data at rest. This includes both data within their data processing facility and also data that might be mobile, such as laptops, mobile devices such as smart phones, and USB Drives. Providers and hospitals must attest that they have done this as part of their risk assessment and may be required to produce documentation if audited (vs. having to affirmatively submit documentation).

Rationale for highlighting encryption at rest: 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 of greater than 500 records. The overwhelming number of these breaches have been caused by thefts or losses of unencrypted data at rest (theft of laptops, servers, portable media, etc.). This is a serious issue that the Tiger Team believes will negatively impact public trust in EHRs if not addressed. Consequently, we believe HHS should use the meaningful use criteria to help address this persistent problem, and highlighting this through meaningful use provides additional policy support for the use of encryption for data at rest.

Another option (2B) is for the Tiger Team to recommend the use of the meaningful use policy lever to encourage providers to specifically address all of the addressable provisions of the HIPAA Security Rule. This would cast a broader net on security and include encryption of data at rest but not highlight it. Providers and hospitals could use the HIPAA Security Rule checklist distributed by ONC through the RECs to help them execute this requirement.

2B. Specifically require, as part of stage 2 of meaningful use, that eligible providers and hospitals address implementation of all addressable provisions of the HIPAA Security Rule. Providers and hospitals must attest that they have done this as part of their risk assessment and may be required to produce documentation if audited (vs. having to affirmatively submit documentation).

Rationale/Issues: This option addresses the full complement of HIPAA Security Rule addressable provisions. The downside to presenting this recommendation is that if CMS takes the same approach to Stage 2 as it did to Stage 1 (not wanting to go beyond HIPAA in the privacy and security category), this faces an uphill battle at being included in Stage 2. This is also arguably the case for option 2A – but the problem of getting providers to encrypt data at rest, and the mistrust this generates among members of the public, may be effective at convincing CMS to “shine a spotlight” on this particular problem.

We note that the Standards Committee has jurisdiction to recommend additional technical functionalities that may be needed in Stage 2 of meaningful use to help support providers and hospitals in complying with the HIPAA Security Rule.

As a final note, regardless of which, if any, of the above options chosen by the Tiger Team, the HHS Office of Civil Rights is the body responsible for interpreting and enforcing the HIPAA Security Rule.

Adam Greene of the HHS Office of Civil Rights, which now enforces both the HIPAA Privacy and Security Rule, has talked recently about the role that certified EHRs play in determining HIPAA security rule compliance. Many of the EHR security capabilities are relevant to “addressable” provisions of the Security Rule. An addressable provision – for example, encrypting data at rest and in motion – is not per se required; if implementing the provision is not “reasonable and appropriate,” an entity can choose an equivalent protection if it is “reasonable and appropriate” (and these decisions must be documented). Recently (for example, at the 2011 HIMSS Annual Meeting), Adam has 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 hard time convincing regulators that it was reasonable for them not to implement it. Consequently, another option for the Tiger Team is to rely on OCR to enforce the security rule, ideally consistent with the notion that users of certified EHRs may face a higher set of expectations with respect to addressable security rule provisions.

Policies for Patient Portals (which have been proposed for Stage 2 of meaningful use)

Related Meaningful Use Objective: patient engagement category (copies of data upon request, access to electronic PHI)

1. **[Insert Tiger Team Recommendations on identity and authentication of patients – see separate document for guidelines/recommendations]**
2. **Eligible Providers and Hospitals should deploy audit trails for access to 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.**

The Markle’s Blue Button Initiative consensus policies and practices included a number of recommended functionalities for a download function in a patient portal. The initial two are security-related and tied to portal functionality; the others arguably should be considered for portals in Stage 2 but may need to be passed along to the Information Exchange workgroup for consideration:

3. **Patient portals:**
 - a. **Should include provisions for data provenance**
 - i. Option: Markle suggested time, date and source stamps for key data entries (such as diagnoses) within information contained in the portal).
 - ii. Option: PCAST recommends data provenance in metadata tags
 - b. **Should include mechanism to prevent automated services (like PHRs) from requiring individuals to provide their user name and password in order to facilitate an automated download.** Standards Committee can set any required standards or functionalities.

Other recommended policies/requirements for portals with a download function:

- c. **Patients must be able to download the information in human readable form.**
- d. **Portal must include a printer-friendly format.**

- e. **Portal must enable the data to be exported into commonly used software formats, such as spreadsheets, pdfs, or text files. Expectation is that migration to more standard formats can occur as they become available and more broadly implemented.**
- f. **Providers and entities offering portals should provide basic education to patients about use of portal, risks and responsibilities (for Tiger Team to take up later – not as time-sensitive because not tied to technical functionality)**