DRAFT: 3/29/11

DRAFT: Additional Privacy and Security Policy Recommendations 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

Topics covered:
-Entity authentication/digital certificates
-Individual User Authentication
-Patient matching/demographic data fields
-Security risk assessment and implementation of EHR security functionalities
-Additional security functionalities required for stage 2 of certification
-Patient portals

Policies to Facilitate Secure Exchange of ePHI among Providers/Hospitals/Laboratories/E-Prescribing Vendors

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 Tiger Team's previous recommendations**

   -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.**

   -For e-prescribing of controlled substances, stage two certification testing criteria for EHRs should include testing of compliance with the DEA authentication rule, which requires two-factor authentication.

Policies to Promote Accurate Patient Matching

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

3. Eligible Providers [and hospitals?] are require 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 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 two 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.**

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.**

2. [**To be determined by the Tiger Team – Whether to add a recommendation regarding implementation of the security functionalities that are required for certified EHRs:** access control, emergency access, auto log-off, audit log, verification that ePHI has not been altered in transit (integrity); authentication (see previous recommendations); and encryption of data at rest and in motion.

Set forth below are four options for recommendation #2 (each discussed in more detail below):

(1) Recommend that eligible providers and hospitals specifically address implementation of certified EHR functionalities.

(2) Rely on OCR's interpretation of how users of certified EHRs must comply with addressable HIPAA security rule provisions
(3) Specifically <u>require</u> implementation of encryption of data at rest.
(4) Specifically <u>require</u> implementation of a full complement of certified EHR security functionalities.

Further discussion of each of the above options:

(1) Recommend that eligible providers and hospitals, as part of their security risk assessment for stage 2 of meaningful use, specifically address how they will implement the security functionalities in the certified EHRs. Providers can 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)

Last year, the Privacy and Security Working Group recommended (and the Policy Committee agreed) that eligible providers and hospitals, as part of this meaningful use risk assessment, should be required to specifically address how the EHR security capabilities will be utilized. <u>One option is for the Tiger Team to recommend this again for Stage 2</u>.

However, CMS did not adopt this recommendation and instead retained just the requirement to perform the required risk assessment under the HIPAA Security Rule. In the final Stage 1 meaningful use rule, CMS stated "we do not see meaningful use as an appropriate regulatory tool to impose different, additional, and/or inconsistent privacy and security policy requirements from those policies already required by HIPAA."

(2) Rely on the Office of Civil Rights to interpret how the HIPAA Security Rule applies to users of certified EHRs.

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.

(3) Specifically require, as part of stage 2 of meaningful use, that eligible providers and hospitals specifically implement the requirement to encrypt data at rest. Providers and hospitals would be required to attest to this as part of Stage 2 of meaningful use

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 HHS could use the meaningful use criteria to address, and highlighting this through meaningful use provides additional policy support for the use of encryption for data at rest. This recommendation could be combined with any of the other option for implementing the other security functionalities.

(4) Specifically require, as part of stage 2 of meaningful use, that eligible providers and hospitals specifically implement a full complement of security policies linked to certified EHRs.

A fourth option for the Tiger Team is to recommend that eligible providers and hospitals be required to implement specific security measures. This option provides more certainty – but 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. Here is an example of required security implementations for meaningful use stage 2; these provisions were taken verbatim from a set of recommendations developed by the Privacy and Security Working Group of the Standards Committee. Presumably this would be measured through provider and/or hospital attestation.

Specifically, Eligilble Providers and Eligible Hospitals must implement policy, procedures and system configuration necessary to use the certified EHR meaningfully, including:

- **Termination of system access of terminated workforce members**
- **Establishment and periodic review of accesses to assure that access is granted to those with permission, and that access is not granted to those who do not have permission**
- **Protection against, detection, and reporting of malicious software***
- **Monitoring of audit trail of system activities***
- **Password-management (if passwords are used for user authentication)***

- **Screen-locking and session termination after pre-established periods of inactivity***
- **Secure hash function to protect the integrity of all PHI transmissions***
- **Encryption of all PHI transmissions, internal or external to the organization, where the possibility of their going over unsecured wireless or cellular networks cannot be ruled out**
- **Encryption of all PHI transmissions that leave the facility and travel in part over shared networks**
- **Encryption of all PHI stored on portable devices and removable media**
- **Update and implement Contingency Plan (data backup plan, disaster recovery plan, emergency-mode operations plan, testing and revision procedures, applications and data criticality analysis) that incorporates use of the EHR product**
- **Identify and document data and capabilities that are minimally required in order to assure continuity of critical data services, and establish service-level-agreements (SLAs) consistent with these priorities**

***items may require additional EHR security functionality (see below)

Additional EHR Security Functionalities

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

The list of security implementation requirements set forth in option 3 above, and developed by the Privacy and Security Working Group of the HIT Standards Committee, includes some requirements that may need to be supported by additional security functionalities in EHRs (see starred requirements above; those not starred are supported by functionalities already in the certification criteria for Stage 1 or do not require technological support). Consider whether the following should be added to the certification criteria for Stage 2:

- Malicious software detection
- Screen locking and session termination after a period of inactivity
- Audit trail processing
- Password management support (for example, see patient authentication recommendations)
- Secure hash function to protect transmissions within an entity? (current integrity standard protects only exchanges of information)
- Others?

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 draft 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)