



Privacy and Security Tiger Team Meeting

Discussion Materials

Today's Topics

- **Notices of Proposed Rulemaking (NPRMs) Related to Stage 2 Meaningful Use**

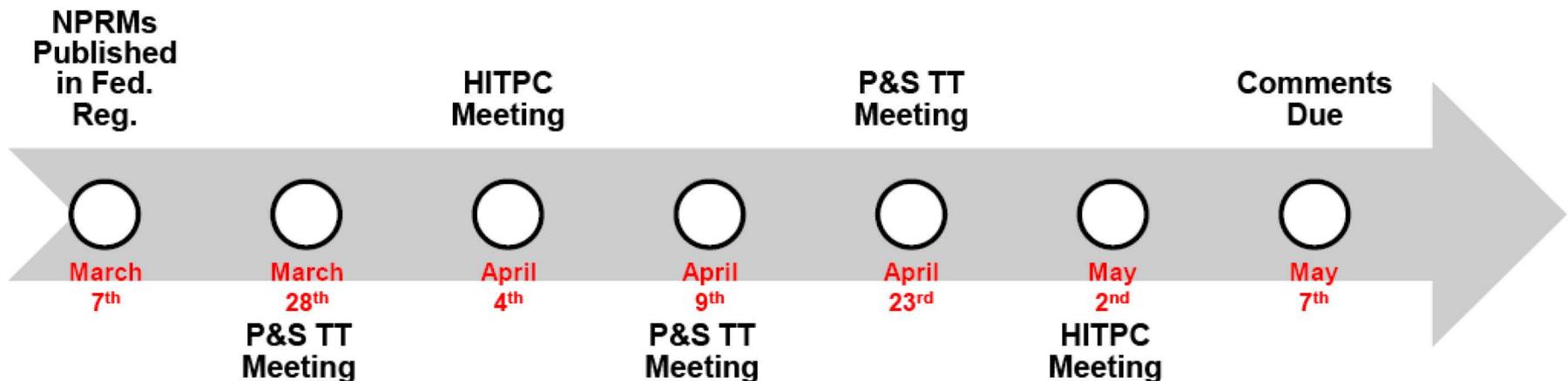
March 19, 2012

Agenda

- Introductory remarks and welcome back
- Scope of Discussion and Timeframes
- Objectives of this Discussion
- Overview of the Proposed Rules
- Issues for Discussion
- Next Meeting

Scope of Discussion and Timeframes

- Notices of proposed rulemaking (NPRMs) related to Stage 2 Meaningful Use:
 - Medicare and Medicaid Programs; Electronic Health Record Incentive Program
 - Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology



Objectives of this Discussion

- Reach agreement on comments to be provided on the proposed rules
- Comments could potentially address:
 - Areas of agreement with the proposed rules
 - Gaps in addressing Tiger Team/HITPC recommendations
 - Aspects of the proposed rules that impact privacy/security

Overview of Rules

- Many Tiger Team/HITSPC recommendations were adopted, for example:
 - ✓ Security Risk Assessment, including encryption at rest
 - ✓ Amendments
 - ✓ Patient Portal: accessible logs, secure third-party download
- Others were not adopted, for example:
 - Digital certificates
 - Authentication for patient portals
- Other issues:
 - No privacy/security certification for EHR modules

Security Risk Analysis and Encryption

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>Stage 1 MU requires EPs and EHs to conduct or review a security risk analysis. This measure should also be included in Stage 2 MU. (HITPC 4/18/11 p. 5)</p>	<p>Conduct or review a security risk assessment. (pp. 82-83)</p>	<p>We do not believe that EHR technology would be able to capture that a security risk analysis was performed by an EP, EH, or CAH except through a manual entry by the EP, EH, or CAH affirming the completion of the risk analysis. (p. 38)</p>	<p>None; recommendation adopted.</p>
<p>Providers/hospitals must address encryption/security functionalities for data at rest, which includes data located in data centers and data in mobile devices. Providers and hospitals must attest that they have done this. (HITPC 4/18/11 p. 6)</p>	<p>Conduct or review a security risk assessment, including addressing the encryption of data at rest. (pp. 82-83)</p>	<p>Perform transmissions which provide for encryption and integrity protection. (p. 28)</p>	<p>None; recommendation adopted.</p>

Amendments

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>Certified EHR technology should have the capability to support amendments, including a provider's compliance with HIPAA requirements to respond to patient requests for amendments:</p> <p>Make amendments to the patients health information in a matter consistent with the entity's obligations w/r/t the legal medical record (i.e., ability to view the original data and identify changes)</p> <p>Append information from the patient and any rebuttal from the entity regarding the data. (HITPC 7/25/11 p. 2)</p>	<p>Not addressed</p>	<p>Enable a user to electronically amend a patient's health record to:</p> <p>(A) Replace existing information/preserves the original; and</p> <p>(B) Append patient supplied information, in free text or scanned, directly to a patient's health record or by embedding an electronic link</p> <p>(ii) Enable a user to electronically append a response to patient supplied information. (p. 173)</p> <p>We specifically request comment on whether EHR technology should be required to be capable of appending patient supplied information in both free text and scanned format or only one or these methods to be certified to this proposed certification criteria. (p. 26)</p>	<p>Recommendation adopted. TT may consider providing comments on whether EHR technology should be required to be capable of appending patient supplied information in free text or scanned format, or both.</p>

Amendments (continued)

Recommendation	MU Stage 2	Certification	Discussion Topics
Certified EHR technology should have the ability by MU Stage 3 to transmit amendments, updates, or appended information to other providers to whom the data has been previously transmitted. (HITPC 7/25/11 p. 2)	Not addressed	Not addressed	None; recommendation could be addressed in Stage 3.

Patient Portals

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>EPs/EHs should deploy audit trails for a patient’s portal, and at least, be able to provide these to patients upon request. (HITPC 4/18/11 p. 5)</p>	<p>Not addressed</p>	<p>EHR technology certified to this criterion include a “patient accessible log” to track the use of the view, download, and transmit capabilities. (pp. 29 – 30; p. 176)</p>	<p>None; recommendation adopted.</p>
<p>Patient portals should include mechanisms that ensure information in the portal can be securely downloaded to a third party authorized by the patients. (HITPC 4/18/11 p. 6)</p>	<p>More than 10 percent of all unique patients seen by the EP, EH or CAH view, download or transmit to a third party their health information. (p. 159)</p>	<p>The ability to transmit a summary care record to a third party. (p. 27)</p> <p>For transport, two standards are available, consistent with the Direct Project - SMTP/SMIME and SOAP. (p. 28)</p> <p>We did not include additional capabilities, such as secure download, in our proposals because we believe their technical implementations are commonplace and ubiquitous. Thus, there would seem to be little value added by requiring that these capabilities be demonstrated as a condition of certification.” (p. 30)</p>	<p>TT may wish to discuss the proposal concerning “secure download.”</p>

Patient Portals (continued)

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>Patient portals should include appropriate provisions for data provenance, which is accessible to the user, both with respect to access and upon download. (HITPC 4/18/11 p. 5)</p>	<p>Not addressed</p>	<p>“...our policy goals can be accomplished through the adoption of the Consolidated CDA standard. This approach also addresses the HITSC’s recommendation for this certification criterion to include ‘data provenance’ with any health information that is downloaded.” (pp. 34-35)</p>	<p>Recommendation adopted? The Consolidated CDA prescribes standard formats, for example, for Author (created content), Data Enterer (transferred content to clinical document), Informant (source of content), Legal Authenticator (single person legally responsible for the document), etc. (HL7 Implementation Guide for CDA 2.1.1 – 2.1.7)</p>

Patient Portals (continued)

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>Certified EHRs should include a capability to detect and block programmatic attacks or attacks from known but unauthorized persons (such as auto lock-out after a certain number of unsuccessful log-in attempts). (HITPC 4/18/11 p. 5)</p>	<p>“...implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.” (p. 83)</p>	<p>Certification criterion should provide some of the basic technical tools necessary to comply with the HIPAA Privacy Rule. (p. 26)</p>	<p>The HITSC's Privacy and Security Workgroup commented: In considering the potential implications of this policy for EHR technology, the Workgroup concluded that this objective/measure does not align well with today's security technology, such as technology that allows entities to federate user identity, (e.g., OpenID, OAuth, SAML). We recommend that the HITSC ask the HITPC to reconsider this objective/measure as a potential “guidance” or “good practice” statement rather than as policy to be implemented in EHR technology.</p>

Patient Portals (continued)

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>Providers should require at least a user name and password to authenticate patients. 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. (HITPC 4/18/11 p. 5)</p>	<p>Not addressed</p>	<p>HITSC recommended that we require as a condition of certification other privacy and security oriented capabilities such as single factor authentication and secure download. We did not include these additional capabilities in our proposals because we believe their technical implementations are commonplace and ubiquitous. Thus, there would seem to be little value added by requiring that these capabilities be demonstrated as a condition of certification. (p. 30)</p>	<p>P&S TT may consider whether to comment.</p>

Patient Portals: Best Practices

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>Note: P&S TT provided best practices (as opposed to certification criteria) on providing guidance to patients using the view and download functionality. (HITPC 8/16/11 pp. 3-4)</p>	<p>The HIT Policy Committee recommended best practice guidance for providers, vendors, and software developments. We believe the hospital can sponsor education and awareness activities that result in patients viewing their information. (p. 147)</p>	<p>Not addressed</p>	<p>P&S TT may wish to underscore reference to the best practices in its comments.</p>

Patient Matching and Demographics

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>HITSC should identify standard formats for data fields that are commonly used for matching patients (for ex: name, DOB, zip, address, gender) (HITPC 4/18/11 p. 8)</p>	<p>EPs/HPs must record the following demographics as structured data:</p> <ul style="list-style-type: none"> - Preferred Language - Gender - Race - Ethnicity - Date of birth - Date and preliminary cause of death in the event of mortality (HPs only) (p. 156) 	<p>Enable a user to electronically record, change, and access patient demographic data including preferred language, gender, race, ethnicity, and date of birth; date and preliminary cause of death (HPs only) (p. 114)</p> <p>We request public comment on whether we should require, as part of the “incorporate summary care record” certification criterion, that EHR technology be able to perform some type of demographic matching or verification between the patient in the EHR technology and the summary care record about to be incorporated. This would help prevent two different patients summary care records from being combined. (p. 59 – 60)</p>	<p>Recommendation adopted?</p> <p>Although the rules do not specifically address the data fields needed for patient matching, the Consolidated CDA prescribes standard formats for name, gender, address, date of birth, telephone number, and zip code contained in the document header; these fields are required. TT may wish to discuss this further. P&S TT may also wish to consider whether to provide comments on the need for certification criteria for demographic matching between the EHR technology and the summary care record.</p>

Patient Matching and Demographics (continued)

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>HITSC should specify standards that describe how missing demographic data should be represented during exchange. (HITPC 4/18/11 p. 8)</p>	<p>“If a patient declines to provide one or more demographic elements, this can be noted in the Certified EHR Technology...” (p. 63)</p>	<p>Not addressed</p>	<p>Recommendation adopted The Consolidated CDA prescribes a series of “null flavors” to designate missing information, for example, NI (no information) and ASKU (asked but not known). These “null flavors” <i>may</i> be used to address required fields. TT may wish to discuss this further.</p>
<p>HITSC should consider whether USPS normalization would be beneficial to improved matching accuracy and whether it should be added to the demographic standards. (HITPC 4/18/11 p. 8)</p>	<p>Not addressed</p>	<p>Not addressed</p>	<p>Recommendation adopted The Consolidated CDA prescribes standards for entering addresses and zip codes. It is our understanding, however, that addresses have not been normalized. TT may wish to discuss this further.</p>
<p>Certification criteria should include testing that (i) appropriate transactions are sent/received with correct demographic data formats and (ii) data entry sequences exist to reject incorrectly entered values. (HITPC 4/18/11 p. 9)</p>	<p>Not addressed</p>	<p>Not addressed</p>	<p>P&S TT may consider whether to comment.</p>

EHR Modules

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>To enable the certification process to more effectively address security integration, the Workgroup recommends that the ONC and National Institute of Standards and Technology (NIST) consider modifying the certification process so that each privacy and security certification criterion is treated as “addressable.” To meet the criterion, each Complete EHR or EHR Module submitted for certification would need to either: (1) implement the required security functionality within the complete EHR or EHR module(s) submitted for certification; or (2) assign the function to a third-party security component or service, and demonstrate how the certified EHR product, integrated with its third-party components and services, meets the criterion.</p> <p>(HITSC 10/21/11 p. 3)</p>	<p>Not addressed</p>	<p>We propose not to apply the privacy and security certification requirements at §170.550(e) for the certification of EHR Modules to the 2014 Edition EHR certification criteria. Stakeholder feedback, particularly from EHR technology developers, has identified that this regulatory requirement is causing unnecessary burden (both in effort and cost). Based on our proposal that EPs, EHs, and CAHs must have a Base EHR to meet our proposed revised definition of CEHRT that would apply beginning with FY/CY 2014, we believe that we can be responsive to stakeholder feedback with our proposal to not to apply the privacy and security certification requirements at § 170.550(e) for the certification of EHR Modules, while still requiring an equivalent or higher level of privacy and security capabilities to be part of CEHRT (p. 125)</p>	<p>P&S TT may wish to consider whether to raise the issue of revisions to EHR Module certification requirements.</p>

E-Prescribing Controlled Substances

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>EPs are required to comply with the DEA rule regarding e-prescribing of controlled substances.</p> <p>Certification testing criteria should include testing of compliance with the DEA authentication rule, which requires 2-factor authentication.</p> <p>(HITPC 4/18/11 p. 3)</p>	<p>Not included: Some challenges remain including more restrictive State law and widespread availability of products that include the functionalities required by the DEA's regulations. We encourage comments addressing the current and expected availability of these products and whether the availability would be sufficient to include controlled substances. (p. 54)</p>	<p>Not addressed</p>	<p>Rules and measures do not at present address e-prescribing of controlled substances. P&S TT may consider responding to request for comments on the availability of products to support e-prescribing of controlled substances.</p>

Digital Certificates

Recommendation	MU Stage 2	Certification	Discussion Topics
<p>EPs and EHs should be required to obtain digital certificates per previous P&S TT recommendations. EHR certification process should include testing on the use of digital certificates for appropriate transactions. (HITPC 4/18/11 p. 3)</p>	<p>Not addressed</p>	<p>Not addressed</p>	<p>P&S TT may consider whether to raise the issue of digital certificates for Stage 2.</p>

Other Issues?

Recommendation	MU Stage 2	Certification	Discussion Topics

Next Meeting

- March 28th
- Continue discussion of proposed rules