



Privacy and Security Tiger Team Meeting

Discussion Materials

Today's Topics

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

April 9, 2012

Today's Discussion

- Objective: Continue efforts to reach agreement on comments to be provided on the proposed rules.
- Presented some recommendations to the HITPC on April 4 (see back-up slides).
- Need to finalize recommendations for Policy Committee meeting on May 2.
- This meeting and one on April 23rd are the only Tiger Team meetings prior to May 2.

Focus of Discussion

- Previous HITPC recommendations not adopted in proposed rules:
 - Patient Portals: secure download, authentication, mechanism to block programmatic or unauthorized attacks; also concerns from HITSC about transparency, security
 - EHR modules
 - E-prescribing of Controlled Substances (EHR capability)
 - Digital certificates: testing of use
 - Patient Matching and Demographics: address normalization, testing of demographic formats

Portals (view/download/transmit)

- Recommendations

1. Require testing of certified EHR technology for authentication of patients (using at least single factor) and secure download
 - Proposed rule states that such technical implementations are commonplace & ubiquitous and therefore do not need to be required for certification
2. Require certified EHR technology to include capability to detect and block programmatic and unauthorized user attacks (note: Standards Committee put forth different recommendation)

Options for comment:

- Reiterate above recommendations and ask that they be included in 2014 certification
- Request OCR develop and issue HIPAA Security Rule Guidance on portals
- Make no comment

Portals (cont.)

- Recommendations

3. Require certified EHR technology to include requirements for data provenance that is accessible to patient/user

Options for Comment

- Addressed by CCDA?
- Reiterate recommendation

4. ONC should provide guidance to providers and hospitals to enable them to be transparent with patients about benefits and risks of portals

Options for Comment

- Urge ONC to more formally endorse guidance recommendations and develop & implement dissemination strategy in preparation for 2014

EHR Modules

- Stage 1 final certification requirements required EHR modules to be tested for all privacy and security certification requirements (except in certain circumstances)
- Stage 2 proposed rule eliminates this requirement and instead requires the Base EHR to be certified for all privacy and security requirements.
- Standards Committee adopted a different recommendation – implement or demonstrate capability to achieve through integration

Background: Base EHR Definition

“A Base EHR can be satisfied through a certified Complete EHR, a single EHR Module, or a combination of certified EHR Modules where the resultant combination has been collectively certified to all of the certification criteria specified in Table below.”

Base EHR Capabilities	Certification Criteria
Includes patient demographic and clinical health information, such as medical history and problem lists	Demographics, Vital Signs, Problem List, Medication List, Medication Allergy List
Capacity to provide clinical decision support	Drug-Drug, Drug-Allergy Interaction Checks, Clinical Decision Support
Capacity to support physician order entry	Computerized Provider Order Entry
Capacity to capture and query information relevant to health care quality	Clinical Quality Measures
Capacity to exchange electronic health information with, and integrate such information from other sources	Transitions of Care, View, Download, and Transmit to 3rd Party
Capacity to protect the confidentiality, integrity, and availability of health information stored and exchanged	Privacy and Security

EHR Modules (cont)

Options for Comment

- No comment; defer to Standards Committee to address
- No comment; compliance with HIPAA Security rule should suffice
- Comment by endorsing Standards Committee approach
- Comment by:
 - Underscoring the risks associated with not requiring compliance with privacy and security criteria and
 - Reiterating recommendation that default approach be that EHR modules must meet all of the privacy and security criteria

E-Prescribing of Controlled Substances

- Recommendations

- Policy Committee recommended that certified EHR Technology have capability to support such 2 factor authentication as required by DEA interim final rules
- ONC declined to propose for Stage 2, noting potential policy conflicts with state law and challenges with widespread ability of products that include functionalities to support DEA requirements
- ONC requests comment on availability point.

- Options for Comment

- Re-assert recommendation – either for Stage 2 or for Stage 3
- Rely on market demand (and other efforts) for Stage 2 and address need to require through certification for Stage 3

Digital Certificates

- Recommendations

1. Policy Committee recommended entity-level digital certificates issued with high degree of assurance
2. Committee also recommended that certified EHR technology be tested on use of such certificates for appropriate transactions.

Options to Address:

- Re-assert recommendation
- Comment that ONC should be sure that the transport standards (and potentially NwHIN governance) address the entity authentication needs raised by the Policy Committee

Patient Matching

- Recommendations

1. Standardization of demographic data fields, including fields for missing data
 2. Consider U.S.P.S. Normalization
 3. Certification should test that (1) appropriate transactions are sent/received with the correct demographic data formats and (2) data entry sequences exist to reject incorrectly entered values.
- Data standards (including those for missing data) exist in CCDA but EHRs are not required to be tested as recommended. No response on normalization recommendation.
 - ONC also requested comments on whether EHR technology should be certified to perform demographic matching.

Patient Matching (cont.)

Options to Address:

- Re-assert some or all recommendations
- Comment that we assume CCDA demographic data fields address the concerns we raise?
 - Use opportunity to also urge ONC to implement address all patient matching recommendations

Backup Slides

Tiger Team Suggestions for Policy Committee Comments on Proposed Rules (1)

- Comment favorably on CMS' proposal to include the security risk assessment (currently in Stage 1) and attesting to addressing encryption of data at rest in Stage 2 as privacy and security MU criteria
- With respect to amendments, comment favorably on ONC's proposal to require that Certified EHR Technology have the capability to make amendments to a patient's health data and be able to append information from the patient & any rebuttal from the entity regarding the data (per HIPAA requirements).
 - EHR Technology should be required to append patient-supplied information in both free text and scanned formats (specific question from ONC).

Tiger Team Suggestions for Policy Committee

Comments on Proposed Rules (2)

- Request that ONC signal in the final Stage 2 rule that by Stage 3 of MU, Certified EHR Technology must demonstrate the capability to transmit amendments (plus appended information) to other providers
- Comment favorably on ONC's proposal to require patient accessible log in Stage 2 certification

Amendments

HITPC Recommendation:

- 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:
 - Make amendments to the patients health information in a matter consistent with the entity's obligations with regard to the legal medical record (i.e., ability to view the original data and identify changes).
 - Append information from the patient and any rebuttal from the entity regarding the data.

Amendments (continued)

Proposed Rule(s):

- Certification NPRM states that certified Complete EHRs and EHR modules must have the capability to:
 - Enable a user to electronically amend a patient's health record to:
 - Replace existing information in a way that preserves the original information; and
 - Append patient supplied information, in free text or scanned, directly to a patient's health record or by embedding an electronic link to the location of the content of the amendment.
 - Enable a user to electronically append a response to patient supplied information in a patient's health record.

Amendments (continued)

- Also **specifically requests 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 of these methods to be certified to this proposed certification criteria.

Comment Options:

- Tentative decisions reached at previous meeting:
 - Comment praising ONC for adopting recommendation on patient amendments; and
 - Comment that the technology should be required to append patient-supplied information in both free text and scanned formats.

Amendments (continued)

HITPC Recommendation (Not Adopted):

- 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 in question has been previously transmitted.
 - Recommendation was narrow in scope and intended only to enable providers to transmit amendments, updates, or appended information to other providers as required by law or as desired by providers.
 - It was not intended, for example, to require that the technology have the capability to identify recipients with whom the information was shared.

Speaker's Note: Certified EHR Technology should have the ability by Meaningful Use Stage 3 to transmit amendments, updates or appended information to other providers to whom the data in question has been previously transmitted.

Patient Portals (View/Download/Transmit)

HITPC Recommendations:

- Patient portals should include mechanisms that ensure information in the portal can be securely downloaded to a third party authorized by the patients.
- Providers should require at least a user name and password to authenticate patients. This single factor authentication should be a minimum.

Patient Portals (continued)

Proposed Rules:

- MU Rule
 - More that 10 percent of all unique patients seen by the EP, EH, or CAH, view, download or transmit to a third party their health information.
- Certification Rule
 - Certified EHRs must have the ability to transmit a summary care record to a third party
 - ONC did not include capabilities for single factor authentication and secure download, stating that such technical implementations are commonplace and ubiquitous and thus, little value would derive by requiring these capabilities as a condition of certification.

Patient Portals (continued)

HITPC Recommendation (Not Sure):

- Patient portals should include appropriate provisions for data provenance, which is accessible to the user, both with respect to access and upon download.

Proposed Rules:

- Certification rule asserts that the adoption of the Consolidated CDA standard addresses the recommendation to include “data provenance” with any health information that is downloaded.
- CDA prescribes standard formats for Author, Data Enterer, Legal Authenticator, etc.

Speaker's Note: 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).

EHR Modules

HITPC Recommendation (Not Adopted):

- In commenting on Stage 1 MU NPRM, the [Privacy and Security Workgroup](#) (precursor to the P&S Tiger Team) strongly endorsed a default rule that all EHR modules must meet all privacy and security certification criteria.

Speaker's Note: See HITPC Recommendations at link; April 2010 meeting.

EHR Modules (continued)

Related HITSC Recommendation

- To enable the certification process to more effectively address security integration, the P&S Workgroup recommends that the ONC and 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:
 - Implement the required security functionality within the complete EHR or EHR module(s) submitted for certification; or
 - Assign the function to a 3rd party security component or service, and demonstrate how the certified EHR product, integrated with its third-party components and services, meets the criterion.

EHR Modules (continued)

Proposed Rules:

- Certification NPRM:
 - Proposes not to apply the privacy and security certification requirements for the certification of EHR Modules, citing stakeholder feedback, particularly from EHR technology developers, that identified that this regulatory requirement is causing unnecessary burden (both in effort and cost).
 - ONC stated: 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 not to apply the privacy and security certification requirements to EHR modules, while still requiring an equivalent or higher level of privacy and security capabilities to be part of CEHRT.

E-prescribing Controlled Substances

HITPC Recommendation (Not Adopted):

- EPs are required to comply with the DEA rule regarding e-prescribing of controlled substances. Certification testing criteria should include testing of compliance with the DEA authentication rule, which requires 2-factor authentication.

E-prescribing Controlled Substances (continued)

Proposed Rule(s):

- MU NPRM:
 - Some challenges remain including more restrictive State law and widespread availability of products that include the functionalities required by the DEA's regulations.
 - **Encourages comments** addressing the current and expected availability of these products and whether the availability would be sufficient to include controlled substances.

Digital Certificates

HITPC Recommendation (Not Sure):

- 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.

Patient Matching and Demographics

HITPC Recommendations:

- HITSC should:
 - Identify standard formats for data fields that are commonly used for matching patients (for ex: name, DOB, zip, address, gender)(Not Sure),
 - Specify standards that describe how missing demographic data should be represented during exchange (Not Sure), and
 - Consider whether USPS normalization would be beneficial to improved matching accuracy and whether it should be added to the demographic standards (Not Adopted).
- Certification criteria should include testing that (1) appropriate transactions are sent/received with correct demographic data formats and (2) data entry sequences exist to reject incorrectly entered values (Not Adopted).

Speaker's Note: Any SHALL conformance statement may use nullFlavor, unless the attribute is required.

Patient Matching and Demographics (continued)

Proposed Rules:

- Certification NPRM:
 - Adopted the Consolidated CDA as a requirement, which includes:
 - standards for name, gender, address, date of birth, telephone number, and zip code contained in the document header and
 - “null flavors” to designate missing information, which may be used to address required fields.
 - Did not address normalization and testing.
 - **Requested public comment** on whether ONC 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.