



# 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**

**March 28, 2012**

# Agenda

- Opening Remarks
- Objectives of this Discussion
- Issues for Discussion
- Next Meeting

# Announcement – New ONC Guidance to State HIE Grantees

- [http://healthit.hhs.gov/portal/server.pt/gateway/PTARG\\_S\\_0\\_0\\_5545\\_1488\\_17157\\_43/http%3B/wci-pubcontent/publish/onc/public\\_communities/\\_content/files/onc\\_hie\\_pin\\_003\\_final.pdf](http://healthit.hhs.gov/portal/server.pt/gateway/PTARG_S_0_0_5545_1488_17157_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/onc_hie_pin_003_final.pdf)
- Provides guidance to state grantees and requires them to submit privacy and security frameworks
- The guidance “builds from the privacy and security and governance recommendations of the Health IT Policy Committee...”
- Includes adoption of policies based on ONC’s articulation of fair information practices and consent

# Today's Discussion

- Objective: Reach agreement on comments to be provided on the proposed rules.
- Time is probably not sufficient to reach agreement on all issues; goal is to present some recommendations to the HITPC on April 4.
- Recommendations fall into three categories:
  - Fully adopted: require no further discussion, victory dance optional,
  - Not Sure: require further discussion drawing on the technical expertise of members also on the Standards Committee to clarify status, and
  - Not adopted: require in-depth discussion.

# Status of Recommendations

- Fully adopted:
  - Security Risk Assessment, including encryption at rest
  - Amendments: support amendments, updates & appended information (Note: Does not include transmission; see following page)
  - Patient Portals: patient accessible log
- Not Sure:
  - Patient Portals: data provenance
  - Patient Matching: standard formats for fields used for matching, missing data
  - Digital Certificates: use of digital certificates

# Status of Recommendations

- Not adopted
  - Amendments: transmission
  - Patient Portals: secure download, authentication, programmatic attacks
  - EHR modules
  - E-prescribing Controlled Substances
  - Digital certificates: testing of use
  - Patient Matching and Demographics: address normalization, testing of demographic formats

# 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.

## Amendments (continued)

### Proposed Rule(s):

- Not addressed in either rule.
- Outstanding question for TT discussion: Does the adoption of transport standards address this capability?

### Comment Options:

- No comment.
- Comment that:
  - It is important that certified technology enable providers to propagate amendments, updates, and appended information to other providers, consistent with existing requirements.
  - The preamble for final rule should include language clearly signaling ONC's intention to require this capability in Stage 3.

# 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)

## Comment Options:

- No comment
- Comment
  - While technical implementations of secure download and single-factor authentication may be widespread, these capabilities should be required as a condition of certification to ensure that they are included in all EHR technology and continue to be available into the future.
  - One of our goals in recommending these capabilities be included as certification criteria was to have them tested.
  - Reiterate recommendations to include these capabilities as a condition for certification in Stage 2.

## 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.

Notes: 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).

## Patient Portals (continued)

### Comment Options:

- No comment; defer to Standards Committee.
- Praise ONC for adopting the Consolidated CDA standard, as it addresses the need for data provenance with downloaded health information.
- Praise ONC for adopting the Consolidated CDA standard but raise any specific areas in which the standard does not go far enough in addressing data provenance.

## Patient Portals (continued)

HITPC Recommendation (Not adopted):

- 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).

# Patient Portals

## Proposed Rule(s)

- Not addressed in either rule.
- Note: The HITSC's Privacy and Security Workgroup considered the HITPC's recommendation on blocking programmatic attacks
  - 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)
  - Recommended 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.

# Patient Portals

## Comment Options

- No comment
- Comment by
  - Referencing Standards Committee views on this recommendation and
  - Recommending that ONC cite this capability as a best practice in the preamble to the final rule.
- Comment by
  - Referencing Standards Committee views on this recommendation and
  - Reiterating recommendations that this be included in certification criteria. (Need rationale)

# Patient Portals

## HITPC Recommendation (Not Sure):

- Best practices—as opposed to certification criteria—for providers, vendors, and software developments for providing guidance to patients using the view/download functionality.

## Proposed Rule(s):

- MU NPRM notes this recommendation and states hospitals can sponsor education and awareness activities that result in patients viewing their information.

# Patient Portals (continued)

## Comment Options:

- No comment.
- Comment by
  - Reiterating the importance of patient education on the use of the view/download capability to encourage protection of the information and
  - Recommending that ONC reference recommendation on guidance in the preamble to the final rule and commit to provide such guidance through, for example, its Regional Extension Center (REC) program.

# 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.

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.

## EHR Modules (continued)

### Comment Options:

- No comment; defer to Standards Committee to address.
- Comment by endorsing Standards Committee recommendation as a way of addressing compliance burden, while providing appropriate privacy and security protections.
- Comment by
  - Underscoring the risks associated with not requiring compliance with privacy and security criteria and
  - Reiterating recommendation that EHR modules must meet all privacy and security certification criteria.

# 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.

## E-prescribing Controlled Substances (continued)

### Comment Options:

- No comment; or
- Comment that sufficiently developed technology should be available by the time that MU rules go into effect; ONC should require this capability as part of Stage 2 certification requirements; or
- Comment that the needed technology may not be available by the time that MU rules go into effect; ONC should, however, strongly signal in the preamble that this capability will be a requirement for Stage 3.

# Digital Certificates

## HITPC Recommendation (Not Sure):

- EPs and EHRs 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.

## Digital Certificates (continued)

### Proposed Rule(s):

- Not addressed in either rule.
- Outstanding question for TT discussion: Do required transport standards require use of digital certificates?

### Comment Options:

- No comment; or
- Comment by highlighting the importance of digital certificates for authentication and reiterating recommendation.

Note: I have been unable to get an answer to the question of whether the transport standards require use of digital certificates.

# 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).

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.

Note: I am still obtaining additional information on how to interpret the standard’s use of nullFlavors.

## Patient Matching and Demographics (continued)

### Comment Options:

- Standards for data fields used for matching
  - No comment/defer to Standards Committee, or
  - Praise ONC for adopting the Consolidated CDA, which should facilitate patient matching, or
  - Praise ONC for adopting the Consolidated CDA, but comment on any standards needing revision.
- Normalization
  - No comment, or
  - Re-emphasize the importance of address normalization and recommend that ONC include address normalization as part of certification.

## Patient Matching and Demographics (continued)

- Testing
  - No comment, or
  - Re-emphasize the importance of testing as part of the certification process and recommend that the final rule include testing as recommended by the HITPC.
- Comments on demographic matching by EHR technology
  - No comment, or
  - Agree that, as part of the “incorporate summary care record” certification criterion, that EHR technology be able to perform demographic matching between the patient in the EHR technology and the summary care, or
  - Disagree that demographic matching should be included in the “incorporate summary care record” certification criterion.

# Next Meeting

- April 4<sup>th</sup> HITPC Meeting
- April 9<sup>th</sup> P&S TT Meeting
  - Continue discussion of proposed rules

# BACKUP SLIDES

# HIPAA Privacy Rule Requirements: Propagate Amendments/Appended Information

Individuals have the right to have Covered Entities (CEs) amend their protected health information (PHI) in a designated record set when that information is inaccurate or incomplete.

*If* a CE accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it; and

To persons that the CE knows might rely on the information to the individual's detriment.

A CE must amend PHI in its designated record set upon receipt of notice to amend from another CE.