



The Office of the National Coordinator for  
Health Information Technology



# Health IT Policy Committee

## Request for Comment Summary

February 20, 2013



- RFC posted on ONC website November 16, 2012, comment period closed January 14, 2013 at 11:59pm - 60 days
- ONC staff has been vigorously working to review and summarize comments
- February 6<sup>th</sup> HITPC
  - High level review of public comments
  - Feedback from the HITSC
- Following HITPC meeting, workgroups will conduct a deep dive of public comments and HITSC feedback



The Office of the National Coordinator for  
Health Information Technology



# Meaningful Use

Michelle Consolazio Nelson  
Meaningful Use Workgroup Lead



- 606 Comments
- Types of organizations that commented
  - Allied professional organizations
  - Consumer organizations
  - EHR consultants
  - Eligible hospitals
  - Eligible professionals
  - Federal agencies
  - Other (e.g. REC community, individual citizens)
  - Payers
  - Provider organizations (clinician and institutional)
  - Vendors
  - Vendor trade groups

- Focus on clinical outcomes in Stage 3
  - Empower flexibility to foster innovation, limiting the scope of recommendations
  - Too much focus on functional objectives
  - Recommendations are too prescriptive
- Concerns about timing
  - Experience needed from stage 2 before increasing thresholds, accelerating measures, or moving from menu to core
  - Concerns about the readiness of standards to support stage 3 goals
- Address interoperability limitations
- Meaningful Use is one component of provider responsibilities
  - Continue to invest in quality measurement alignment, infrastructure and standards
- Ensure that patient safety remains a high priority and any related requirements are synchronized with Meaningful Use
- Make use of all technology available, everything does not need to happen in the EHR
- Many commenters were confused by certification criteria only items

ID#	Summary
MU 01	<p data-bbox="195 396 1702 486"><b>Is there flexibility in achieving a close percentage of the MU objectives, but not quite achieving all of them?</b></p> <ul data-bbox="220 508 1783 779" style="list-style-type: none"><li data-bbox="220 508 537 544">• 75 Comments</li><li data-bbox="220 568 1783 779">• Most commenters urged the HITPC to recommend more flexibility in the MU program<ul data-bbox="316 629 1750 779" style="list-style-type: none"><li data-bbox="316 629 1244 665">• Flexibility will be important for full year reporting</li><li data-bbox="316 689 1750 779">• Recommendations that providers be considered in compliance if they meet 75 percent of the objectives</li></ul></li></ul>

ID#	Summary
MU 02	<p data-bbox="195 396 1789 482"><b>What is the best balance between ease of clinical documentation and the ease of practice management efficiency?</b></p> <ul data-bbox="220 508 1798 939" style="list-style-type: none"><li data-bbox="220 508 537 544">• 59 Comments</li><li data-bbox="220 568 1798 654">• Most commenters favored improvements in overall usability that could be expected to make this balance more manageable.</li><li data-bbox="220 678 1653 714">• Natural language processing (NLP) was identified as an usability improvement,</li><li data-bbox="220 738 1760 823">• Possibility to reallocate practice workflow to evenly distribute the work and increase overall practice efficiency</li><li data-bbox="220 848 1740 933">• There were a number of statements that the question was beyond the scope of the Meaningful Use program</li></ul>

ID#	Summary
MU 03	<p><b>To improve the safety of EHRs, should there be a MU requirement for providers to conduct a health IT safety risk assessment? Are there models or standards that we should look to for guidance?</b></p> <ul style="list-style-type: none"><li>• 63 comments</li><li>• Overwhelming opposition to a MU requirement as premature, but support for the need for EHR users to do a safety assessment</li></ul>

ID#	Summary
MU 06	<p><b>What can be included in EHR technology to give providers evidence that a capability was in use during the EHR reporting period for measures that are not percentage based.</b></p> <ul style="list-style-type: none"><li>• 48 Comments</li><li>• Commenters generally agree that EHRs should be able to track usage for yes/no measures</li><li>• Many suggested that the audit log would be an appropriate functionality for tracking usage and that providers should have only 'read-access' to the log</li><li>• Commenters equally noted the difficulty in tracking activities that occur in the EHR and those that occur outside the EHR</li></ul>



The Office of the National Coordinator for  
Health Information Technology



# Information Exchange

Kory Mertz  
Information Exchange Workgroup Lead



HealthIT.gov

ID#	Summary
IEWG01	<p data-bbox="202 335 637 371"><b>Query for patient record</b></p> <ul data-bbox="202 392 1864 1278" style="list-style-type: none"><li data-bbox="202 392 531 428">• 102 comments</li><li data-bbox="202 449 1700 492">• Many commenters expressed support for the inclusion of this objective in Stage 3.</li><li data-bbox="202 514 1864 656">• Quite a few commenters seemed confused about the focus and scope of this objective. Many seemed to think it was focused on requiring providers to utilize a HIO leading to concerns about the level of access to fully functional HIOs.</li><li data-bbox="202 678 1758 771">• Quite a few commenters expressed the need to complete additional work around the privacy and security implications of this objective.</li><li data-bbox="202 792 1758 878">• A number of commenters stated that HIE/HIOs should be able to support providers in achieving this objective.</li> <li data-bbox="202 963 1816 1049">• <i>Measure:</i> The majority of those who commented on the measure suggested it should be based on a percentage. Requested additional detail on how the measure will be calculated.</li> <li data-bbox="202 1135 1835 1278">• <i>Patient matching:</i> A few commenters on this objective requested ONC establish explicit standards to support patient matching. A few commenters felt it was important to establish a national patient identified to support correctly matching patients for this objective.</li></ul>

ID#	Summary
IEWG0 2	<p data-bbox="241 332 568 372"><b>Provider directory</b></p> <ul data-bbox="241 394 1792 605" style="list-style-type: none"><li data-bbox="241 394 552 434">• 62 comments</li><li data-bbox="241 455 1792 544">• Most commenters agreed that there are not sufficiently mature standards in place to support this criteria at this time.</li><li data-bbox="241 565 1673 605">• Comments were fairly evenly split on if the criterion should be kept in Stage 3.</li></ul>
IEWG0 3	<p data-bbox="241 636 523 676"><b>Data portability</b></p> <ul data-bbox="241 698 1846 1229" style="list-style-type: none"><li data-bbox="241 698 552 738">• 56 comments</li><li data-bbox="241 759 1823 848">• The majority of commenters felt this criterion was important and that further progress needed to be achieved around data portability.</li><li data-bbox="241 869 1846 1009">• Requests for a variety of data elements to be added common themes were to ensure new data elements included in Stage 3 be added to this criterion and that any historical data required to calculate Stage 3 CQMs be included as well.</li><li data-bbox="241 1031 1765 1119">• A number of commenters felt this criterion was unnecessary or duplicative of other criteria.</li><li data-bbox="241 1140 1644 1229">• A few commenters questioned if this criterion would add significant value as substantially more data would need to be migrated to maintain continuity.</li></ul>

ID#	Summary
MU05	<p>The HITECH ACT has given a lot of emphasis to EHRs as the central distribution channel for health information, but there may be limits on how much we can add on to EHR technologies. As additional program demands are added onto EHRs, what can be done to foster innovation to share information and receive intelligence from other, non-EHR applications and services that could be built on top of that data architecture?</p> <p>For example, Is it possible to create an application programming interface (API) to make available the information defined in a CCDa so that systems can communicate it with each other? Is the information defined in the CCDa the appropriate content for other uses of clinical information? Are the standards used to communicate between EHR systems (e.g. Direct, Exchange) adequate for communication between EHRs and other kinds of systems? What other technologies, standards or approaches could be implemented or defined to facilitate the sharing of clinical knowledge between EHRs and other systems?</p> <ul style="list-style-type: none"><li>• 78 comments</li><li>• There were many suggestions for what can be done to foster innovation. Key Points that were identified in the comments were:<ul style="list-style-type: none"><li>• Implement standard interface specification to support integration for the EHRs and other systems</li><li>• Differing views on CCDa and Direct and Exchange ability to communicate between EHRs and other kinds of systems.</li><li>• Believe that publishing of healthcare APIs will speed the development of truly integrated systems</li></ul></li></ul>



The Office of the National Coordinator for  
Health Information Technology



# Privacy and Security

Will Phelps  
Privacy and Security Workgroup Lead



HealthIT.gov

# PSTT01 Summary:

## Re-use of 3rd Party Credentials

**PSTT01 - How can the HITPC's recommendation be reconciled with the National Strategy for Trusted Identities in Cyberspace (NSTIC) approach to identification which strongly encourages the re-use of third party credentials?**

- 41 comments received
- Many comments state that strong identity proofing and multi-factor authentication should be required for MU3 and that the NSTIC Model can be adopted in healthcare
  - Existing standards such as NIST SP 800-63, CIO Council Guidance, FEMA, and OMB, and DEA standards are suggested for consideration
- Some comments do not believe that multi-factor authentication should be required for MU3 citing that:
  - The deadline to implement is unrealistic
  - The requirement would introduce burden and increased costs, especially on small providers
  - Multi-factor authentication is not a core competency of EHRs

# PSTT02 Summary:

## Certification Criteria for Testing Authentication

### **PSTT02 - How would ONC test the HITPC's recommendation (for two-factor authentication) in certification criteria?**

- 26 comments received
- Comments suggest possible approaches including:
  - Developing a checklist to verify the system set-up, while also requiring appropriate documentation
  - Requiring vendors to attest to having an architecture that supports third-party authentication and demonstrate examples
  - Checking for use of a federation language standard
  - Developing a model audit protocol for the community to use to self-test
  - Developing an iterative and phased testing program covers the population of organizations
- Existing standards and guidance that could be the basis of test procedures include:
  - DEA Interim Final Rule (IFR)
  - NIST 800-63
  - FIPS 201
  - HSPD-12
  - NSTIC/Identity Ecosystem Accreditation Standards
- One comment suggests that the domain is not mature enough for certification

# PSTT03 Summary: EHR Certification - Standalone or w/3rd Party

## **PSTT03 - Should ONC permit certification of an EHR as stand-alone and/or an EHR along with a third-party authentication service provider?**

- 30 comments received
- Many comments support both models
- Several comments suggest the EHR and third-party authentication service be certified independently of each other
- Logistic suggestions for the two models include:
  - Third-party dependencies could be handled the same way that database and operating system dependencies are handled in sectors such as the Payment Card Industry
  - In lieu of requiring certification ONC could implement NSTIC
  - Certification could be carried out to an ONC recognized healthcare trust framework by an NSTIC Accreditation Authority
  - Use external labs capable of and experienced in testing identity and authentication technologies in accordance with FIPS 201 for third party authentication providers

# PSTT04 Summary: MU Attestation for Security Risks

**PSTT04 - What, if any, security risk issues (or Health Insurance Portability and Accountability Act (HIPAA) Security Rule provisions) should be subject to Meaningful Use attestation in Stage 3?**

- 46 comments received
- Workforce security training:
  - Comments for - cite the importance of the workforce in keeping health information secure
  - Comments against - cite attestation is either burdensome or duplicative of the HIPAA Security Rule
- Safeguard and training areas to emphasize include:
  - Access controls
  - Audits
  - Data integrity
  - Encryption
  - Identity management
  - Implementation of backup and recovery plans
  - Policies and procedures related to prevention of local PHI storage
  - Malware on all workstations accessing EHRs and EHR modules
  - Social media, bring your own device (BYOD), and mobile devices
  - Local data storage security controls
- Some comments say more HIPAA Security Rule guidance and education is needed for providers

# PSTT05 Summary: Certification Standard for Audit Logs

**PSTT05 - Is it feasible to certify the compliance of EHRs based on the prescribed [ASTM] standard for [audit logs]?**

- 30 comments received
- Majority of comments state prescribed standard is feasible
- Many comments focus on whether or not there should be a standard
  - Many comments suggest there should not be a standard yet
  - Some comments suggest MU standards premature until final Accounting of Disclosures Rule issued
  - Some comments say question implies combining audit log and accounting of disclosures requirements
    - Audit logs require more information than necessary for an accounting of disclosures

**PSTT06 - Is it appropriate to require attestation by meaningful users that such logs are created and maintained for a specific period of time?**

- 37 comments received
- Comments suggest waiting until the Accounting of Disclosures Rule requirements are finalized before addressing attestation
- Comments supporting attestation also suggest other audit log requirements
  - Be able to certify a separate audit log system
  - Rely on NIST/Federal or State regulation
  - Incorporate into risk assessment
  - Credential users
  - Base on standards that give guidance for content
  - Specify period of time
  - Identify a minimum data set
- Other comments suggest attestation to all requirements in the HIPAA Privacy and Security Rules

- Majority of comments are neutral toward attestation requirements, citing a need to:
  - Wait for final Accounting of Disclosures Rule
  - Complete additional feasibility studies/research
  - Leverage audit log requirements in other industries
  - Defer to providers and hospitals for feedback
- Some comments do not support attestation requirements, citing:
  - Administrative burden
  - Need to also require demonstrating function
  - No improvement to security
  - Audit log is functionality of EHR, not a provider attestation requirement

# PSTT07 Summary: Standard Format for Log Files

**PSTT07 - Is there a requirement for a standard format for the log files of EHRs to support analysis of access to health information access multiple EHRs or other clinical systems in a healthcare enterprise?**

- 32 comments received
- Many comments state that there is no adequate standard format requirement
- Most comments support a need for standard format requirement
- Some comments are neutral toward standard format requirement, suggesting that:
  - Government should dictate what but not how
  - Variability on details captured presents a challenge to creating a standard
  - Use of SIEM standard
- Some comments disagree with need for standard format requirement
  - Requirement elements can be mandated and should define a minimum data set
  - Burden on health care organizations and vendors
- Some comments state there is no need for MU based standards related to Accounting of Disclosures Rule

# PSTT08 Summary: Audit Log File Specifications

**PSTT08 - Are there any specifications for audit log file formats that are currently in widespread use to support such applications?**

- 37 comments received
- Some comments mention specifications that could be considered for audit log purposes, such as:
  - IHE ATNA Specification
  - HL7
  - DICOM
  - ASTM E E-2147-01
  - World Wide Web Consortium (W3C)
  - SYSLOG
  - UNIX-based operating systems
- Some comments state there are no existing standards or no existing standards in widespread use
- Other comments oppose new MU requirements based on proposed rule

**MU4: Some federal and state health information privacy and confidentiality laws, including but not limited to 42 CFR Part 2 (for substance abuse), establish detailed requirements for obtaining patient consent for sharing certain sensitive health information, including restricting the recipient's further disclosure of such information. *Three questions were put forth.***

- 74 comments received
- ***Question 1: How can EHRs and HIEs manage information that requires patient consent to disclose so that populations receiving care covered by these laws are not excluded from health information exchange?***
  - Approaches suggested include:
    - Metadata tagging
    - Data segmentation , such as...
      - Data Segmentation for Privacy Initiative
      - VA/SAMHSA
      - SATVA
  - Concerns expressed:
    - The necessary segmentation capabilities do not exist today
    - It is better to focus on identifying and punishing inappropriate use of data
    - Use PHR to give patients control of their data

- ***Question 2: How can MU help improve the capacity of EHR infrastructure to record consent, limit the disclosure of this information to those providers and organizations specified on a consent form, manage consent expiration and consent revocation, and communicate the limitations on use and restrictions on re-disclosure to receiving providers?***
  - Create and adopt standards to improve the capacity of EHR infrastructure
  - Create standardized fields for specially protected health information
  - Require all certified EHRs manage patient consent and control re-disclosure
- ***Question 3: Are there existing standards, such as those identified by the Data Segmentation for Privacy Initiative Implementation Guide, that are mature enough to facilitate the exchange of this type of consent information in today's EHRs and HIEs?***
  - Many comments call attention to segmentation-related initiatives that might be leveraged , such as:
    - S&I Framework's Data Segmentation for Privacy Initiative (DS4P WG)
    - HL7 confidentiality and sensitivity code sets
    - SAMHSA/VA pilot
    - eHI developed the "eHealth Initiative Blueprint: Building Consensus for Common Action"

- Outcome of February 6<sup>th</sup> HITPC discussion, exploring alternative pathways
  - Performance based deeming
  - Clustering /consolidating objectives
- March 15<sup>th</sup> in-person meeting to explore options
- April 3<sup>rd</sup> will review details with HITPC