# Charge to the Certification and Adoption Workgroup

At the January 8, 2013 HITPC meeting, Jodi Daniel gave a presentation on the Health Information Technology Patient Safety Action & Surveillance Plan (aka Safety Plan) which is out for public comment on healthit.gov. The Certification and Adoption Workgroup has been asked to provide comments on the Safety Plan related to the focused questions listed below.

# Focused Questions (questions underlined below)

### Meaningful Use and Safety Risk Assessment

* To improve the safety of EHRs, should there be a Meaningful Use requirement for providers to conduct a health IT safety risk assessment?
* Are there models or standards that we should look to for guidance

(These two bullets have been submitted for public comment)

### Meaningful Use and Reporting

* Should ONC require any form of reporting/reporting verification under Meaningful Use?

### Standards and Certification Criteria Next Steps

The Health IT Safety Plan states that *“ONC intends to continue using its standards and certification criteria and certification program rulemaking in ways that enhance health IT patient safety, focusing on human factors, safety culture, and user - centered design (Page 17).”*

In the 2014 Edition EHR certification criteria final rule, ONC took the steps below to improve usability and patient safety.

1. Certified EHR technology developers will be required to publicly identify a method of incorporating user - centered design of eight certification criteria that have a high likelihood of helping to prevent medical errors (77 Fed Reg 54186-54189 (September 4, 2012)).
2. Certified EHR technology developers will also be required to provide transparency regarding their approach to “quality management systems,” (77 Fed Reg 54189-54191 ((September 4, 2012))

* What should be the next steps in terms of EHR technology certification?

**Initial feedback summary (from comments received by ONC):**

* There is overwhelming opposition to a MU requirement. It is seen as premature.
* There is support for the need for EHR users to complete a safety assessment.
* Many noted the absence of a safety assessment tool.
* In regard to tools ; the HIPAA Security Rule, Leapfrog assessment, and ISMP assessment were identified.

**Position of CHIME is representative of the comments received so far:**

*“CHIME believes it would be premature to impose a health IT safety risk assessment requirement at this time. We believe that doing so could have a chilling effect, since EPs and EHs are already challenged by other meaningful use requirements. We instead urge the Department to continue to pursue other initiatives, such as dissemination of best practices regarding HIT use, mining adverse event reports for useful information and making it easier for clinicians to report patient safety events and risks using EHR technology, incorporating safety into certification criteria for HIT products (as was done with the Stage 2 certification criteria relating to user-centered design and quality management systems), and funding relevant research and pilot projects. We believe these alternatives would be more fruitful in the near-term than imposition of yet another regulatory requirement.”*

**Key Points**

* Overwhelming “No” on MU requirement for a safety risk assessment beyond what is already required in the Security Rule risk assessment.
* Primary Reason:  Doing so is premature.  Absence of clear tools for doing a HIT safety assessment, although many comments acknowledged that progress is being made in this area.  Many were aware of ONC’s efforts, including development of tools and the HIT Patient Safety Action and Surveillance Plan.
* Many comments embraced importance of EHR safety, even as they said no to a MU requirement for a health IT safety risk assessment.
* Many comments supported a public-private process to develop health IT safety standards/measures.  Many encouraged development of best practices.
* The HIPAA Security rule, Leagfrog assessment and Institute for Safe Medication Practices (ISMP), were identified as potential tools.
* Several comments emphasized need to incorporate health IT safety assessment into an overall culture of safety, not as separate process.
* Many identified need for reporting of health IT-related events, and suggested this could be built into EHRs.
* As tools are developed, should focus on high risk areas.  Importance of CDS safety assessment was identified in several comments.
* Several provider comments identified need for safety assessment as part of certification of EHRs, seeing Stage 3 as continued focus on what vendors should do in product development to ensure health IT safety.
* Several comments focused on health IT safety as a “shared responsibility”.
* One comment focused on burden on small practices without significant IT resources.

**January 31, 2013 Workgroup Discussion**

* Presentation - Health Information Technology Patient Safety Action & Surveillance Plan

- David Hunt, ONC

* Discussion by Workgroup members

**Summary of Workgroup Discussion:**

One concern was raised concerning these new potential requirements is any additional burden on the EP.  Even a single click for measurement or any interruption in workflow is unacceptable.  Any requirements should be on the vendors to make reporting easier or direct from the technology, but there should be no additional requirements placed on users, other than a possible requirement to report any incident that actually has occurred.

Topics discussed include:

1. Provider conducted self-assessment of patient safety risks, including HIT – ONC is working on guidelines for this, the Safer Guides, expected in September of 2013.
2. Provider identification events and associated data capture (including unsafe conditions and near misses). AHRQ Common Formats.
3. Protected pathway for reporting and analysis within the provider organization.
4. Mechanism for reporting to PSO (I think we can be this specific in the reporting methodology)
5. Built into vendor products – likely will be more than a “button” since not all events are that simple, but a “button” might be a good place to start – there may be “apps for that” including the ONC Challenge winner

**MU objective**: Providers attest that they conduct a health IT safety risk assessment (e.g., using SAFER guide) and have policies and procedures in place for users to report potential safety risks or incidents in a convenient, efficient manner.

**Certification criteria (agree with ONC proposed plan):** Certified EHR technology developers will be required to publicly identify a method of incorporating user - centered design of eight certification criteria that have a high likelihood of helping to prevent medical errors (77 Fed Reg 54186-54189 (September 4, 2012)).

1. *CPOE*
2. *Drug-drug, drug-allergy interaction checks*
3. *Medication list*
4. *Medication allergy list*
5. *Clinical decision support*
6. *Electronic medication administration record*
7. *Electronic prescribing*
8. *Clinical information reconciliation*

Certified EHR technology developers will also be required to provide transparency regarding their approach to "quality management systems," (77 Fed Reg 54189-54191 ((September 4, 2012))

**ADD**:

* Certified EHRs have a convenient mechanism for EHR users to report safety risks or incidents (not limited to perceived EHR-related risks) they observe using the AHRQ Common Format. The EHR automatically captures the EHR context in which the user is creating the report (e.g., activity, screen, patient [patient context is important for internal investigation, but the information would be de-identified before submitting elsewhere], other EHR context).
* Certified EHR technology developers must transmit customer-reported safety submissions to a designated Patient Safety Organization.

*AHRQ's Common Formats include:*

* *Event descriptions (descriptions of patient safety events and unsafe conditions to be reported),*
* *Specifications for patient safety aggregate reports and individual event summaries,*
* *Delineation of data elements to be collected for different types of events to populate the reports,*
* *A users guide and quick guide, and*
* *Technical specifications for electronic data collection and reporting*

**Background About SAFER: Safety Assurance Factors for EHR Resilience**  
As part of its ongoing commitment to patient safety in electronic health record (EHR)-enabled healthcare systems, the Office of the National Coordinator for Health Information Technology (ONC) sponsored the November 2011 Institute of Medicine report, “*Health IT and Patient Safety: Building Safer Systems for Better Care,*” and an expert panel on negative unintended consequences that may result from rapid EHR adoption.   As an outgrowth of those efforts, this project, referred to as SAFER: Safety Assurance Factors for EHR Resilience, will develop a series of guides outlining best practices to be used by a variety of stakeholders in both the inpatient and ambulatory environments.  Areas to be addressed by the guides include  
   
   The ordering process, including computerized provider order entry (CPOE) and e-prescribing  
   System customization/configuration and upgrades  
   System to system interfaces such as that between CPOE and pharmacy systems  
   Patient identification processes  
   Clinical decision support  
   Provider communication during transitions of care  
   Laboratory results review processes  
   Downtime events  
   HIT safety-related human skills  
   High priority principles and practices for EHR safety