American Hospital Association

Regulatory Advisory

August 26, 2010

ONC Final Rule on Certification Criteria and Standards for EHRs

AT A GLANCE

The Issue:

The Office of the National Coordinator for Health Information Technology (ONC) on July 28 in the *Federal Register* published a final rule establishing an initial set of standards, implementation specifications, and certification criteria for electronic health record (EHR) technology. At the same time, the Centers for Medicare & Medicaid Services (CMS) issued a final rule establishing the requirements for meaningful use of EHRs. Taken together, these regulations set EHR adoption requirements that hospitals and physicians must meet under the *American Recovery and Reinvestment Act of 2009* to qualify for additional Medicare and Medicaid incentive payments beginning in fiscal year 2011 and to avoid significant payment penalties in 2015 and later years.

This advisory addresses ONC's final rule on certification criteria and standards. The certification final rule from ONC, which takes effect August 27, can be viewed at http://edocket.access.gpo.gov/2010/pdf/2010-17210.pdf. An AHA *Regulatory Advisory* on CMS' final rule on EHR incentives and meaningful use is available at http://www.aha.org/aha/advisory/2010/100813-regulatory-adv.pdf. This rule can be viewed at http://edocket.access.gpo.gov/2010/pdf/2010-17207.pdf; it takes effect September 27.

Our Take:

In the rule, ONC finalized a definition of certified EHRs and a related initial set of certification criteria, standards and implementation specifications. The certification criteria follow the Stage 1 meaningful use objectives laid out by CMS and also require specific capabilities to protect the privacy and security of health information. The ONC certification criteria and standards primarily address the highly technical requirements for certification of EHR technology by vendors or those hospitals and physicians that want to certify self-developed technology. The final rule also affects other hospitals and physicians, however, because some of the meaningful use criteria established in the CMS rule require use of the standards adopted by ONC. In addition, all providers that want to receive the meaningful use incentives and avoid later penalties must use certified EHR technology.

What You Can Do:

- ✓ Share this advisory with your senior management team.
- ✓ Ask your chief information officer to examine how this final rule will affect your plans to implement EHRs and achieve meaningful use.
- ✓ Consult AHA's Regulatory Advisory on CMS' final rule on meaningful use, as well as the ONC final rule for the certification process.
- ✓ Consult additional AHA educational materials, including information on individual topics in meaningful use (www.aha.org/hitcalls) and the recent *Hospitals in Pursuit of Excellence Leadership Guide to EHR Implementation* (www.hpoe.org/compendium/index.shtml).

Questions:

If you have questions or need more information, please contact Chantal Worzala, director of policy, at (202) 626-2313 or cworzala@aha.org.

AHA's Regulatory Advisories are produced whenever there are significant regulatory developments that affect the job you do in your community. A 19-page summary of this issue follows.

American Hospital Association

Regulatory Advisory

August 26, 2010

ONC Final Rule on Certification Criteria and Standards for EHRs

TABLE OF CONTENTS

BACKGROUND

The American Recovery and Reinvestment Act of 2009 (ARRA) authorized incentive programs under Medicare and Medicaid that will pay bonuses to "meaningful users" of certified electronic health records (EHR) beginning in fiscal year (FY) 2011, then phase-in penalties for those failing to meet "meaningful use" beginning in FY 2015. To be eligible for the incentives, hospitals and physicians must use EHRs that have been certified through a new federal certification process established by the Office of the National Coordinator for Health Information Technology (ONC).

Three regulations will govern the incentive programs:

- A "meaningful use" rule from the Centers for Medicare & Medicaid Services (CMS) that sets out the requirements for hospitals and other providers;
- A rule from ONC on the certification criteria and standards that must be met by vendor products and EHR systems that hospitals and physicians self-develop; and
- A certification process rule from ONC that establishes new certifying bodies for EHRs.

This advisory summarizes key elements of ONC's rule finalizing the certification criteria and standards that are of importance to hospitals and other providers. The final rule modified provisions adopted under an Interim Final Rule (IFR) that took effect February 12, 2010. This advisory does not fully address all of the technical material presented by ONC. Hospitals and other providers in need of additional information, such as those seeking to certify self-developed EHR technology, should consult the regulatory text, which is available at http://edocket.access.gpo.gov/2010/pdf/2010-17210.pdf. The final rule takes effect August 27.

The AHA's advisory on CMS's final rule on meaningful use is available at http://www.aha.org/aha/advisory/2010/100813-regulatory-adv.pdf. This rule can be viewed at http://edocket.access.gpo.gov/2010/pdf/2010-17207.pdf; it takes effect September 27.

The AHA's *Regulatory Advisory* on the third rule establishing the certification process is available at http://www.aha.org/aha/advisory/2010/100720-regulatory-adv.pdf. This rule is available at http://edocket.access.gpo.gov/2010/pdf/2010-14999.pdf and took effect upon publication in the June 24 *Federal Register*.

AS IT STANDS

In the rule, ONC finalizes a definition of certified EHRs and an initial set of certification criteria, standards and implementation specifications for EHRs. The certification criteria follow the Stage 1 meaningful use objectives laid out by CMS and also require specific capabilities to protect the privacy and security of health information. The certification criteria apply to EHR products, not providers. Hospitals and physicians, however, must use certified EHRs to qualify for the Medicare and Medicaid incentive payments.

ONC is establishing a temporary certification program. ONC-Authorized Testing and Certification Bodies (ONC-ATCBs) will conduct testing to ensure that EHRs meet the certification criteria using testing tools approved by ONC. These tools are available at: http://xw2k.nist.gov/healthcare/use_testing/index.html. At present, no certification bodies have been authorized and no certified products are available. ONC expects to approve one or more ONC-ATCBs this fall.

ONC states that the purpose of the final rule is to adopt standards, implementation specifications, and certification criteria to test and certify that EHR technology can, at a minimum, support the achievement of proposed meaningful use Stage 1 by eligible professionals (EPs), eligible hospitals and critical access hospitals (CAHs) under the Medicare and Medicaid EHR Incentive Programs (see AHA's *Regulatory Advisory* on the CMS rule for further details).

The longer term goal of certification generally, and standards adoption particularly, is to enhance the interoperability, functionality, utility and security of health information technology (IT). ONC also anticipates adoption of additional standards, implementation specifications and certification criteria, as well as revisions and updates to those standards initially adopted for future stages of meaningful use.

Definition of Certified EHR Technology

In the rule, ONC provides a multi-stage definition of "certified EHR technology." In essence, providers must use either a "Complete EHR" that was developed to meet, at a minimum, all of the applicable certification criteria adopted by the Secretary of Health and Human Services (HHS), or a combination of EHR Modules developed individually to meet at least one criterion but taken together meet all of the certification criteria adopted by the Secretary for either the ambulatory or inpatient setting. A Complete EHR may or may not include additional capabilities.

In the final rule, ONC clarifies that an EHR Module may provide one or many capabilities, but cannot include all of the capabilities of a Complete EHR. To qualify, it must have at least one capability that is tested and certified to the certification criteria, but may have additional functionalities that do not meet certification criteria for use as part of certified EHR technology.

Providers who choose to combine multiple EHR Modules are responsible for ensuring that the Modules work together and that, together, they meet all of the certification criteria. Providers will have to attest to using certified EHR technology to demonstrate meaningful use under the Medicare and Medicaid EHR Incentive Programs.

Standards and Implementation Specifications

ONC adopts specific standards that fall into three categories:

- Content Exchange Standards, which are standards used to share clinical information such as clinical summaries, prescriptions, structured electronic documents and quality reporting;
- Vocabulary Standards, including standardized nomenclatures, terminology and code sets used to describe clinical problems and procedures, lab test results, medications, immunizations, and race and ethnicity; and
- Privacy and Security Standards, such as encryption and decryption, access control and transmission security, which relate to and span across all of the other types of standards.

In some cases, ONC also adopts an "implementation specification" related to a specific standard defined in the final rule as "specific requirements or instructions for implementing a standard." ONC defines a standard as "a technical, functional, or performance-based rule, condition, requirement, or specification that stipulates instructions, fields, codes data, materials, or actions." In response to comments, ONC removed two specific transport standards it had adopted in the IFR – the Simple Object Access Protocol (SOAP) and the Representational State Transfer (REST).

In some instances, the CMS meaningful use rule requires use of specific standards in order to be a meaningful user. The certification criteria require that vendor systems be able to support these standards, but hospitals and other providers will have to ensure that data are collected or shared in standardized formats. The standards adopted by ONC are listed in Appendix A.

The AHA is currently developing a mapping of requirements across the two rules and seeking clarification from CMS and ONC on the extent to which standards must be used to meet meaningful use. Examples of standards required by CMS include:

- Structured problem lists incorporate ICD-9-CM or SNOMED-CT as standards for diagnoses.
- Race and ethnicity data incorporate the OMB Race and Ethnicity Categories listed in OMB Directive Number 15 (these categories are explained in the AHA/HRET Disparities Toolkit available at www.hretdisparities.org).
- Smoking status incorporates as structured values: current every day smoker, current some-day smoker, former smoker, never smoker, smoker with current status unknown and unknown if ever smoked.
- Providing patients with copies of their electronic health information incorporates a number of specific standards for how the data are coded (vocabulary standards) and structured for exchange (content exchange standards). While data do not need to be collected using these standards, they must be in these formats for exchange. Data will need to be mapped to these standards.

Certification Criteria

The final rule modified many of the certification criteria and associated standards to support the achievement of meaningful use Stage 1. Some of these changes result from changes in the definition of meaningful use; others respond to comments on the current stage of technology and readiness to adopt specific standards.

Table 1 (next page) lists the final certification criteria applicable for meaningful use Stage 1 objectives and measures. Following the structure used by ONC, the table is organized into three panels: certification criteria applicable to both ambulatory and inpatient EHRs; those applicable to inpatient EHRs; and those applicable to ambulatory EHRs. The certification criteria incorporate specific standards through regulatory reference. Readers are referred to Appendix A, where the standards are provided with their regulatory references.

Of special note for hospitals, physicians and other EPs:

- ONC includes certification criteria related to the calculation and submission of all 15 clinical quality measures specified by CMS for eligible hospitals and CAHs. Although the AHA and others urged ONC to include in the certification criteria that EHRs must show they can **accurately** calculate the quality measures, ONC stated in the final rule that it did not believe this was necessary. The AHA is very concerned that the quality metrics reported directly from EHRs will not be scientifically valid and reliable given the lack of field testing for these measures.

- ONC also includes certification criteria related to the calculation and submission of clinical quality measures for physicians and other EPs. However, the certification requirements only include calculation of the three core measures, three alternative core measures, and three of the additional 38 quality measures that physicians may choose to report. This limitation was adopted to ensure that specialty-specific EHRs did not need to calculate measures unrelated to a specific specialty. The AHA is concerned, however, that this limited certification requirement will result in ambulatory EHRs that cannot report the full set of quality measures for EPs, effectively limiting the ability of EPs to choose which measures to report. We are especially concerned about the impact of this policy on hospital outpatient departments, which generally include EPs from many different medical specialties who will want to report quality metrics relevant to their scope of practice.

- As recommended by the AHA and others, ONC clarifies in the rule that the certification criteria include automated measure calculation for each meaningful use objective with a percentage-based measure. This will lower the burden of reporting for providers and eliminate manual calculations.

- As recommended by the AHA and others, the final rule clarifies that conducting medication reconciliation "electronically" means providing a user the ability to electronically compare two or more medication lists. This preserves the role of the clinician in medication reconciliation. The IFR, in contrast, implied that certified EHR technology must automate medication reconciliation.

- As recommended by the AHA and others, the final rule removes requirements for Complete EHRs/EHR Modules to include capabilities to electronically check insurance eligibility and submit claims because CMS removed these objectives from meaningful use Stage 1 requirements. ONC notes that CMS explained in

the final rule on EHR meaningful use that inclusion of administrative simplification requirements as part of Stage 2 is an important long-term policy goal, and ONC announces its intention to include for adoption administrative transactions standards and certification criteria to support meaningful use Stage 2 rulemaking and expects providers and Complete EHRs/EHR Modules developers to take this into account for 2013.

- ONC adopts in the rule certification criteria for two meaningful use Stage 1 objectives added by CMS:

  - Record Advance Directives for Patients 65 Years Old and Older (applicable to Complete EHRs and EHR Modules designed for inpatient settings.)
  - Patient-Specific Education Resources (applicable to Complete EHRs and EHR Modules designed for ambulatory and inpatient settings.)

- Either the ASTM Continuity of Care Record (CCR) or HL7 Continuity of Care Document (CCD) must be used to generate and share summary patient data. Vendor products also must be able to display patient summary information received in either format.

- The eight privacy and security certification criteria are meant to ensure that hospitals and other providers have the tools they need to secure electronic personal health information. A more detailed discussion of the certification criteria for privacy and security follows the table.

Table 1. Certification Criteria to Support Meaningful Use Stage 1

Function	Certification Criteria
Panel 1. General Certification Criteria (Inpatient and Ambulatory)	
Implement Drug-drug and Drug-allergy Interaction Checks	(1) Notifications. Automatically and electronically generate and indicate in real-time, notifications at the point of care for drug-drug and drug-allergy contraindications based on medication list, medication allergy list, and computerized provider order entry (CPOE). (2) Adjustments. Provide certain users with the ability to adjust notifications provided for drug-drug and drug-allergy interaction checks.
Implement Drug-formulary Checks	Enable a user to electronically check if drugs are in a formulary or preferred drug list.
Maintain an Up-to-date Problem List	Enable a user to electronically record, modify, and retrieve a patient's problem list for longitudinal care in accordance with: (1) The [vocabulary] standard specified in §170.207(a)(1); or (2) At a minimum, the version of the [vocabulary] standard specified in §170.207(a)(2).
Maintain Active Medication List	Enable a user to electronically record, modify, and retrieve a patient's active medication list as well as medication history for longitudinal care.
Maintain Active Medication Allergy List	Enable a user to electronically record, modify, and retrieve a patient's active medication allergy list as well as medication allergy history for longitudinal care.
Record and Chart Vital Signs	(1) Vital signs. Enable a user to electronically record, modify, and retrieve a patient's vital signs including, at a minimum, height, weight, and blood pressure. (2) Calculate body mass index. Automatically calculate and display body mass index (BMI) based on a patient's height and weight.

Function	Certification Criteria
	(3) Plot and display growth charts. Plot and electronically display, upon request, growth charts for patients 2-20 years old.
Smoking Status	Enable a user to electronically record, modify, and retrieve the smoking status of a patient. Smoking status types must include: current every day smoker; current some day smoker; former smoker; never smoker; smoker, current status unknown; and unknown if ever smoked.
Incorporate Laboratory Test Results	(1) Receive results. Electronically receive clinical laboratory test results in a structured format and display such results in human readable format. (2) Display test report information. Electronically display all the information for a test report specified at 42 CFR 493.1291(c)(1) through (7). (3) Incorporate results. Electronically attribute, associate, or link a laboratory test result to a laboratory order or patient record.
Generate Patient Lists	Enable a user to electronically select, sort, retrieve, and generate lists of patients according to, at a minimum, the data elements included in: (1) Problem list; (2) Medication list; (3) Demographics; and (4) Laboratory test results.
Medication Reconciliation	Enable a user to electronically compare two or more medication lists.
Submission to Immunization Registries	Electronically record, modify, retrieve, and submit immunization information in accordance with: (1) The [content exchange] standard (and applicable implementation specifications) specified in §170.205(e)(1) or §170.205(e)(2); and (2) At a minimum, the version of the [vocabulary] standard specified in §170.207(e).
Public Health Surveillance	Electronically record, modify, retrieve, and submit syndrome-based public health surveillance information in accordance with the [content exchange] standard (and applicable implementation specifications) specified in §170.205(d)(1) or §170.205(d)(2).
Patient-Specific Education Resources	Enable user to electronically identify and provide patient-specific education resources according to, at a minimum, the data elements included in the patient's: problem list; medication lists; and lab test results; as well as provide such resources to the patient.
Automated Measure Calculation	For each meaningful use objective with a percentage-based measure, electronically record the numerator and denominator and generate a report including the numerator, denominator, and resulting percentage associated with each applicable meaningful use measure.
Access Control	Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information
Emergency Access	Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.
Automatic Log-off	Terminate an electronic session after a predetermined time of inactivity.
Audit Log	(1) Record actions. Record actions related to electronic health information in accordance with the [privacy/security] standard specified in §170.210(b). (2) Generate audit log. Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the [privacy/security] standard at 170.210(b).
Integrity	(1) Message Digest. Create a message digest in accordance with the [privacy/security] standard specified in 170.210(c). (2) Verification. Verify in accordance with the [privacy/security] standard specified in §170.210(c) upon receipt of electronically exchanged health information that such information has not been altered. (3) Detection. Detect the alteration of audit logs.

Function	Certification Criteria
Authentication	Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.
Encryption	(1) General encryption. Encrypt and decrypt electronic health information in accordance with the [privacy/security] standard specified in §170.210(a)(1), unless the Secretary determines that the use of such algorithm would pose a significant security risk for certified EHR technology. (2) Encryption when exchanging electronic health information. Encrypt and decrypt electronic health information when exchanged in accordance with the [privacy/security] standard specified in §170.210(a)(2).
Accounting of Disclosures	Record disclosures made for treatment, payment, and health care operations in accordance with the [privacy/security] standard specified in §170.210(d) [*Optional*]
Panel 2. Criteria Specific to the Inpatient Setting	
Computerized Provider Order Entry	Enable a user to electronically record, store, retrieve, and modify, at a minimum, the following order types: (1) Medications; (2) Laboratory; and (3) Radiology/imaging.
Record demographics	Enable a user to electronically record, modify, and retrieve patient demographic data including preferred language, gender, race, ethnicity, date of birth, and date and preliminary cause of death in the event of mortality. Enable race and ethnicity to be recorded in accordance with the standard specified at § 170.207(f).
Clinical Decision Support	*(1) Implement rules.* Implement automated, electronic clinical decision support rules (in addition to drug-drug and drug-allergy contraindication checking) based on the data elements included in: problem list; medication list; demographics; and laboratory test results. *(2) Notifications.* Automatically and electronically generate and indicate in real-time, notifications and care suggestions based upon clinical decision support rules.
Electronic Copy of Health Information	(1) Enable a user to create an electronic copy of a patient's clinical information, including, at a minimum, diagnostic test results, problem list, medication list, medication allergy list, and procedures: (i) In human readable format; and (ii) On electronic media or through some other electronic means in accordance with: (A) The standard (and applicable implementation specifications) specified in § 170.205(a)(1) or § 170.205(a)(2); and (B) For the following data elements the applicable standard must be used: *(1) Problems.* The standard specified in § 170.207(a)(1) or, at a minimum, the version of the standard specified in§ 170.207(a)(2); *(2) Procedures.* The standard specified in § 170.207(b)(1) or § 170.207(b)(2); *(3) Laboratory test results.* At a minimum, the version of the standard specified in § 170.207(c); and *(4) Medications.* The standard specified in § 170.207(d). (2) Enable a user to create an electronic copy of a patient's discharge summary in human readable format and on electronic media or through some other electronic means.
Electronic Copy of Discharge Instructions	Enable a user to create an electronic copy of the discharge instructions for a patient, in human readable format, at the time of discharge on electronic media or through some other electronic means.
Exchange Clinical Information and Patient Summary Record	*(1) Electronically receive and display.* Electronically receive and display a patient's summary record from other providers and organizations including, at a minimum, diagnostic test results, problem list, medication list, medication allergy list, and procedures in accordance with the standard (and applicable implementation specifications) specified in § 170.205(a)(1) or § 170.205(a)(2). Upon receipt of a patient summary record formatted according to the alternative standard, display it in human readable format. *(2) Electronically transmit.* Enable a user to electronically transmit a patient's summary record to other providers and organizations including, at a minimum,

Function	Certification Criteria
	diagnostic results, problem list, medication list, medication allergy list, and procedures in accordance with: (i) The standard (and applicable implementation specifications) specified in § 170.205(a)(1) or § 170.205(a)(2); and (ii) For the following data elements the applicable standard must be used: (A) *Problems.* The standard specified in § 170.207(a)(1) or, at a minimum, the version of the standard specified in § 170.207(a)(2); (B) *Procedures.* The standard specified in § 170.207(b)(1) or § 170.207(b)(2); (C) *Laboratory test results.* At a minimum, the version of the standard specified in § 170.207(c); and (D) *Medications.* The standard specified in § 170.207(d).
Reportable Lab Results	Electronically record, modify, retrieve, and submit reportable clinical lab results in accordance with the standard (and applicable implementation specifications) specified in § 170.205(c) and, at a minimum, the version of the standard specified in § 170.207(c).
Advance Directives	Enable a user to electronically record whether a patient has an advance directive.
Calculate and Submit Clinical Quality Measures	*(1) Calculate.* Electronically calculate all of the clinical quality measures specified by CMS for eligible hospitals and critical access hospitals. *(2) Submission.* Enable a user to electronically submit calculated clinical quality measures in accordance with the standard and implementation specifications specified in § 170.205(f).
	Panel 3. Criteria Applicable to the Ambulatory Setting
Computerized Provider Order Entry	Enable a user to electronically record, store, retrieve, and modify, at a minimum, the following order types: (1) Medications; (2) Laboratory; and (3) Radiology/imaging.
Electronic Prescribing	Enable a user to electronically generate and transmit prescriptions and prescription-related information in accordance with: (1) The standard specified in § 170.205(b)(1) or § 170.205(b)(2); and (2) The standard specified in § 170.207(d).
Record Demographics	Enable a user to electronically record, modify, and retrieve patient demographic data including preferred language, gender, race, ethnicity, and date of birth. Enable race and ethnicity to be recorded in accordance with the standard specified at § 170.207(f).
Patient Reminders	Enable a user to electronically generate a patient reminder list for preventive or follow-up care according to patient preferences based on, at a minimum, the data elements included in: (1) Problem list; (2) Medication list; (3) Medication allergy list; (4) Demographics; and (5) Laboratory test results.
Clinical Decision Support	(1) *Implement rules*. Implement automated, electronic clinical decision support rules (in addition to drug-drug and drug-allergy contraindication checking) based on the data elements included in: problem list; medication list; demographics; and laboratory test results. (2) *Notifications*. Automatically and electronically generate and indicate in real-time, notifications and care suggestions based upon clinical decision support rules.
Electronic copy of Health Information	Enable a user to create an electronic copy of a patient's clinical information, including, at a minimum, diagnostic test results, problem list, medication list, and medication allergy list in: (1) Human readable format; and (2) On electronic media or through some other electronic means in accordance with: (i) The standard (and applicable implementation specifications) specified in §

Function	Certification Criteria
	170.205(a)(1) or § 170.205(a)(2); and (ii) For the following data elements the applicable standard must be used: (A) *Problems*. The standard specified in § 170.207(a)(1) or, at a minimum, the version of the standard specified in § 170.207(a)(2); (B) *Laboratory test results*. At a minimum, the version of the standard specified in § 170.207(c); and (C) *Medications*. The standard specified in § 170.207(d).
Timely Access	Enable a user to provide patients with online access to their clinical information, including, at a minimum, lab test results, problem list, medication list, and medication allergy list.
Clinical Summaries	Enable a user to provide clinical summaries to patients for each office visit that include, at a minimum, diagnostic test results, problem list, medication list, and medication allergy list. If the clinical summary is provided electronically it must be: (1) Provided in human readable format; and (2) Provided on electronic media or through some other electronic means in accordance with: (i) The standard (and applicable implementation specifications) specified in § 170.205(a)(1) or § 170.205(a)(2); and (ii) For the following data elements the applicable standard must be used: (A) *Problems*. The standard specified in § 170.207(a)(1) or, at a minimum, the version of the standard specified in § 170.207(a)(2); (B) *Laboratory test results*. At a minimum, the version of the standard specified in § 170.207(c); and (C) *Medications*. The standard specified in § 170.207(d).
Exchange Clinical Information and Patient Summary Record	(1) *Electronically receive and display*. Electronically receive and display a patient's summary record, from other providers and organizations including, at a minimum, diagnostic tests results, problem list, medication list, and medication allergy list in accordance with the standard (and applicable implementation specifications) specified in § 170.205(a)(1) or § 170.205(a)(2). Upon receipt of a patient summary record formatted according to the alternative standard, display it in human readable format. (2) *Electronically transmit*. Enable a user to electronically transmit a patient summary record to other providers and organizations including, at a minimum, diagnostic test results, problem list, medication list, and medication allergy list in accordance with: (i) The standard (and applicable implementation specifications) specified in § 170.205(a)(1) or § 170.205(a)(2); and (ii) For the following data elements the applicable standard must be used: (A) *Problems*. The standard specified in § 170.207(a)(1) or, at a minimum, the version of the standard specified in § 170.207(a)(2); (B) *Laboratory test results*. At a minimum, the version of the standard specified in § 170.207(c); and (C) *Medications*. The standard specified in § 170.207(d).
Calculate and Submit Clinical Quality Measures	(1) *Calculate*. (i) Electronically calculate all of the core clinical measures specified by CMS for eligible professionals. (ii) Electronically calculate, at a minimum, three clinical quality measures specified by CMS for eligible professionals, in addition to those clinical quality measures specified in paragraph (1)(i). (2) *Submission*. Enable a user to electronically submit calculated clinical quality measures in accordance with the standard and implementation specifications specified in § 170.205(f).

Privacy and Security Certification Criteria

ONC states that it is important for the privacy and security certification criteria to remain consistent with the HIPAA security rule to the degree that certified EHR technology includes technical capabilities that can assist HIPAA-covered entities in complying with applicable legal requirements. However, ONC suggests that what a HIPAA-covered entity must do to remain in compliance with the HIPAA security rule is separate and distinct from the capabilities that a Complete EHR or EHR Module must include in order to be certified. ONC does not believe that it is precluded by the ARRA from adopting certification criteria that go beyond the requirements specified in the HIPAA security rule. According to ONC, the ARRA directs only that standards, implementation specifications, and certification criteria be consistent with the HIPAA standards, but it simultaneously authorizes the HHS Secretary to adopt certification criteria more broadly for the electronic use and exchange of health information. Thus, ONC specifically rejects any suggestion that its current certification criteria are precluded by the current requirements in the HIPAA security rule.

ONC finalized eight privacy and security certification criteria with associated standards, which address:

- Accounting of disclosures (optional);
- Access control;
- Emergency access;
- Automatic log-off;
- Audit log;
- Integrity;
- Authentication; and
- Encryption.

The specific criteria are included in Table 1. The remainder of this section reviews areas of special interest to hospitals.

Accounting of disclosures. Responding to comments by the AHA and others about the significant technical and policy challenges that remain unresolved, ONC has determined that the certification criterion related to accounting for disclosures for treatment, payment and health care operations will not be a condition of EHR certification at the present time. Instead of removing it completely from the criteria, ONC has made it "optional," keeping the wording of the standard unchanged solely to provide guidance to developers of complete EHRs and modules that choose to adopt this capability at the current time.

This optional criterion (sec. 170.302(w)) continues to read:

> Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in sec. 170.210(d).

Under sec. 170.210(d), the date, time, patient identification, user identification and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined in the HIPAA privacy rule.

However, as ONC clarifies, no Complete EHR or EHR Module will be required to possess this capability for current certification. Additionally, as requested by the AHA, ONC also indicates that it plans to work collaboratively with the Office for Civil Rights (OCR) as OCR develops the regulatory policy related to the ARRA-mandated accounting of disclosures requirement. ONC anticipates updating the certification criterion to reflect OCR's final policies.

Emergency Access. As the preamble makes clear, the "emergency access" criterion is not intended to specify what constitutes an emergency or who would be authorized to access electronic health information in an emergency. Emergency could encompass a clinical or life threatening emergency related to a patient as well as a broader range of possibilities, including normal patient care when timely access to electronic health information becomes critical. Rather, whether an emergency exists and who should be authorized to access information would be based on specific factual circumstances and made in accordance with applicable state and federal laws, organizational policies and procedures, and the relevant standard of care.

ONC believes that this certification criterion is consistent with the HIPAA security rule. Under the HIPAA security rule, emergency access is a necessary part of access controls and, therefore, a required implementation specification of the "access controls" standard. Access controls are still necessary under emergency conditions, although they may differ from controls used in normal circumstances. If normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or manmade disaster, for example, an organization already should have procedures in place to ensure electronic PHI can be accessed.

Audit Log. ONC suggests that audit log capabilities are an essential component of certified EHR technology. The referenced standard requires that the date, time, patient identification, and user identification must be recorded when electronic information is created, modified, accessed or deleted; and an indication of which action(s) and by whom also must be recorded. Audit logs, for example, provide valuable information to eligible professionals and eligible hospitals in the event of a security incident. Audit logs can assist in the identification of security incidents, such as unauthorized access, as well as serve to deter users from conducting fraudulent or abusive activities and detect such activities. Based on ONC's understanding of the current EHR technology in the market, the capabilities specified in the final criterion are common industry practice.

As the preamble notes, auditing of a "printing" action, as the proposed standard envisioned, easily could be circumvented, making the burden of trying to audit accurately any occurrence of printing outweigh any benefit. Accordingly, ONC's final standard does not require logging of printing.

However, although printing is not an auditable action, "access" is an auditable action in the final standard, and ONC specifically understands "access" as encompassing both "reading" or "viewing" despite not referencing those actions explicitly in the standard. As ONC has specified that only certain data must be recorded in the final standard, ONC believes that the specificity will help reduce any potential burden associated with

recording the action “accessed.” ONC also indicates that the action of “accessed” is a superset of actions which may include “export” and, as a result, the final standard does not explicitly reference “export” as some commenters on the proposed rule recommended.

Additionally, in response to comments requesting clarification of the term “user identification” and recommendations for use of existing standards-based definitions, such as HL7's definition of author which includes person, organization, or device, ONC states that:

> The HL7's definition of author is consistent with our expectation. While we believe that in most cases a user will be a health care professional performing an action using Certified EHR Technology, it is also possible that a device or another software process or program could perform any one of these actions. We do not intend to preclude developers of complete EHR or modules from including these and other types of specific features.

ONC also clarifies that the phrase “any of the elements specified by 170.210(b)” would also include, for example, “date” or that information has been “deleted.”

As ONC notes, the purpose of adopted certification criteria is to specify the required capabilities for a Complete EHR or EHR Modules to be certified, not when such capabilities must be used. Accordingly, ONC does not specify in this certification criterion the time period for which an audit log should be “on.”

However, ONC does agree that audit logs should be maintained in a secure manner, and, as a result, preserves the capability adopted in the IFR as part of the “integrity” certification criterion that specified that Certified EHR Technology must be capable of detecting alterations to audit logs (see below). Further, ONC encourages the HIT Standards Committee to consider additional capabilities for audit logs.

Finally, ONC notes that it decided to defer adoption of the IHE Audit Trail and Node Authentication (ATNA) Integration Profile because the standard can be configured in multiple ways. ONC states that it would not be appropriate at this time to require a specific implementation as a condition of certification, but points out that the deferral does not preclude developers of Complete EHRs and EHR Modules from using the ATNA standard.

Integrity. ONC intends for this certification criterion and the related standard (Sec. 170.210(c)) to support, at a minimum, the HIPAA security rule implementation specification (45 CFR 164.312(e)(2)(i)) to “[i]mplement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.” This criterion requires that a hashing algorithm with a security strength equal to or greater than SHA-1 (Secure hash algorithm (SHA-1) as specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-3 (October 2008)) be used to verify that electronic health information has not been altered. ONC states that it is not necessary or appropriate to

address whether hashing is applicable to public and private networks because the adopted criterion specifies a capability that certified technology must include.

Additionally, ONC clarifies that certified EHR technology must include the capability to check the integrity of health information that has been received through electronic exchange, but does not specify the instances in which this capability needs to be executed. According to ONC, certified EHR technology should be capable of generating a hash of electronic health information and, upon receipt of such information, verifying that it has not been altered when it has been electronically exchanged. Nevertheless, in response to proposed rule comments requesting clarity related to this certification criterion, ONC states:

> [W]e expect Certified EHR Technology to be capable of creating a message digest and when in receipt of a message digest, to use the message digest to verify that the contents of the message have not been altered.

However, ONC recognizes that certain situations may not be conducive to the use of hashes and, this is the reason why ONC does not specify the instances in which hashing must be used.

More information on SHA-1 and other secure hash algorithms can be found in FIPS 180-3 at http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf. More information on the security strength of certain hashing algorithms can be found in the National Institute of Standards and Technology (NIST) Special Publication 800-107 at http://csrc.nist.gov/publications/nistpubs/800-107/NIST-SP-800-107.pdf.

However, ONC has not specified a particular standard for detecting alterations to audit logs at this time.

Authentication. Agreeing with concerns raised in comments on the proposed rule, ONC states that "cross-network authentication" should not be a condition of certification at the present time and, consequently, this specific part of the certification criterion and the associated standard has been removed from the final certification criterion for authentication.

Additionally, responding specifically to a request for clarification about whether "user name and password" would be sufficient to authorize a user or whether biometrics would be required, ONC states that "[w]e do not believe that it is appropriate to specify, as a condition of certification, the types of factors that users could utilize to authenticate themselves."

Encryption. ONC requires that certified EHR technology must have the capability of encrypting electronic health information; and the technology must, according to ONC, include the capability to encrypt and decrypt information regardless of the transmission method used. ONC does not specify the policies surrounding the use of encryption by an EP or eligible hospital nor specify that it should apply only to devices. Rather ONC simply intends for certified EHR technology to be technologically capable of encryption,

thereby allowing, if desired or required, an EP or eligible hospital that adopts certified EHR technology to use this capability. Generally, ONC expects the certification criterion will ensure that certified EHR technology is capable of assisting EPs and eligible hospitals to implement more secure technical solutions if they determine, based on their risk analysis, that technical safeguards such as encryption are reasonable and appropriate, or required.

ONC specifically revises the final standard to be more flexible regarding the encryption algorithms certified EHR technology would be permitted to implement. Specifically, Sec. 170.210(a)(1) specifies any encryption algorithm identified by the NIST as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publications 140-2 (incorporated by reference in sec. 170.299).

Because of the flexibility in the final standard, how encryption is technically implemented is left to the developer of the Complete EHR or EHR Module to determine within the parameters of Annex A of FIPS 140-2. The particular changes made to the final general encryption standard, ONC believes, ensure that the full range of the most secure encryption algorithms are available for developers to implement.

ONC points out that the IFR's example list of protocols that would meet the certification criterion was not intended to be exhaustive or to suggest that Complete EHRs or EHR Modules must be capable of using all of the listed protocols to be certified. The example list of protocols was included solely for illustrative purposes. Moreover, ONC simply modifies the standard for encryption when exchanging information to express that the standard is "any encrypted and integrity protected link."

ONC suggests that certified EHR technology capable of encrypting electronic health information will be especially desirable because of the new ARRA-mandated breach notification requirements and the new interim final rule to implement these requirements. As a result, ONC clarifies how the final standard relates to the guidance included in the breach notification interim final rule:

> The National Institute of Standards and Technology (NIST) published Federal Information Processing Standards (FIPS) Publication 140-2 to specify the security requirements for cryptographic modules. As part of FIPS 140-X conformance, NIST publishes "annexes" of different "approved" security protocols. For purposes of encryption, NIST maintains "Annex A" which identifies "approved security functions." Annex A identifies both symmetric and asymmetric key encryption algorithms that NIST has identified for use in accordance with FIPS 140-2. In response to commenters' concerns, we believe that leveraging NIST's work in this area provides for a clearer requirement for compliance and provides Complete EHR and EHR Module developers with the ability to use one or more secure encryption algorithms for the purposes of demonstrating compliance with this certification criterion. We believe this flexibility will benefit eligible professionals and eligible hospitals because they may be able to leverage a broader suite of secure encryption algorithms. As noted in Special Publication 800-111, which is specified in the guidance included

> in the breach notification interim final rule for the encryption of data at rest, "[w]henever possible, AES [Advanced Encryption Standard] should be used for the encryption algorithm because of its strength and speed."

Additionally, ONC notes that the adopted certification criterion permits the HHS Secretary to retain certain discretionary authority with respect to acceptable encryption algorithms. ONC specifically adopts the list of approved encryption algorithms that NIST has identified and referenced in FIPS 140-2 Annex A, and incorporates the list by reference in the final criterion. However, as ONC notes, "while the list is intended to be current, we anticipate that NIST will on an as-needed basis revise and update the list, based on the development of new technologies or perhaps on identified vulnerabilities associated with a particular algorithm." Moreover, ONC states that "[r]egardless of any revisions to this list by NIST, this version of Annex A that is incorporated by reference will remain effective for purposes of serving as the adopted encryption standard." Under the standard as adopted in the final rule, if the Secretary determines that one of the listed encryption algorithms poses a significant security risk for certified EHR technology, the Secretary will notify the public on the department's website (and through the *Federal Register*, although perhaps with some time delay), and will direct ONC-ATCBs or ONC-ACBs not to test and certify complete EHRs and EHR modules using the particular compromised algorithm. HHS then would follow-up with rulemaking as necessary and appropriate to update the adopted list of acceptable encryption algorithms.

NEXT STEPS

Please share this advisory with your senior management team and ask your chief information officer to examine how this final rule will affect your plans to implement EHRs and achieve the certification requirements for meaningful use. Be sure that your medical records department is aware of the standards requirements for collecting data on race and ethnicity, problem lists, and smoking status. Your privacy and security staff also should review those portions of the final rule. If you have not already done so, you or your CIO should discuss with your EHR vendors the products they intend to certify. Assess your need to supplement with additional certified EHR Modules or self-certification to ensure that your system has been fully certified.

Watch for more educational materials, including a mapping between the CMS meaningful use rule and the ONC certification criteria and standards rules, on the AHA's website: www.aha.org.

The AHA is concerned that the intersection of the two rules from CMS and ONC leaves many open questions about the exact set of clinical data systems that must be certified and the standards that must be used by hospitals and physicians to meet the meaningful use criteria. We will be working with members to identify areas of uncertainty and obtain additional guidance from CMS and ONC.

If you have questions, please contact Chantal Worzala, director of policy, at (202) 626-2313 or cworzala@aha.org.

Appendix A: Standards and Implementation Specifications for Health Information Technology, with Regulatory References

§170.205 Content exchange standards and implementation specifications for exchanging electronic health information.

(a) Patient summary record.
(1) Standard. Health Level Seven (HL7) Clinical Document Architecture (CDA) Release 2, Continuity of Care Document (CCD).
- Implementation specifications. The Healthcare Information Technology Standards Panel (HITSP) Summary Documents Using HL7 CCD Component HITSP/C32.

(2) Standard. ASTM E2369 Standard Specification for Continuity of Care Record (CCR) and Adjunct to ASTM E2369.

(b) Electronic prescribing.
(1) Standard. The National Council for the Prescription Drug Programs (NCPDP) Prescriber/Pharmacist Interface SCRIPT standard, Implementation Guide, Version 8, Release 1 (Version 8.1) October 2005.
(2) Standard. NCPDP SCRIPT Standard, Implementation Guide, Version 10.6.

(c) Electronic submission of lab results to public health agencies.
Standard. HL7 2.5.1.
- Implementation specifications. HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 (US Realm).

(d) Electronic submission to public health agencies for surveillance or reporting.
(1) Standard. HL7 2.3.1.
(2) Standard. HL7 2.5.1.
- Implementation specifications. Public Health Information Network HL7 Version 2.5 Message Structure Specification for National Condition Reporting Final Version 1.0 and Errata and Clarifications National Notification Message Structural Specification.

(e) Electronic submission to immunization registries.
(1) Standard. HL7 2.3.1.
- Implementation specifications. Implementation Guide for Immunization Data Transactions using Version 2.3.1 of HL7 Standard Protocol Implementation Guide Version 2.2.

(2) Standard. HL7 2.5.1.
- Implementation specifications. HL7 2.5.1 Implementation Guide for Immunization Messaging Release 1.0.

(f) Quality reporting.
Standard. The CMS Physician Quality Reporting Initiative (PQRI) 2009 Registry XML Specification.
- Implementation specifications. PQRI Measure Specifications Manual for Claims and Registry.

§170.207 Vocabulary standards for representing electronic health information.
(a) Problems.
(1) Standard. The code set specified at 45 CFR 162.1002(a)(1) (relating to ICD-9-CM Volumes 1 and 2) for the indicated conditions.
(2) Standard. International Health Terminology Standards Development Organization (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED-CT®) July 2009 version.

(b) Procedures.
(1) Standard. The code set specified at 45 CFR 162.1002(a)(2) (relating to ICD-9-CM Volume 3 procedures).
(2) Standard. The code set specified at 45 CFR 162.1002(a)(5) (relating to combination of HCPCS and CPT-4).

(c) Laboratory test results.
Standard. Logical Observation Identifiers Names and Codes (LOINC®) version 2.27, when such codes were received within an electronic transaction from a laboratory.

(d) Medications.
Standard. Any source vocabulary that is included in RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine.

(e) Immunizations.
Standard. HL7 Standard Code Set CVX - Vaccines Administered, July 30, 2009 version.

(f) Race and Ethnicity.
Standard. The OMB Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15, October 30, 1997 (available at http://www.whitehouse.gov/omb/rewrite/fedreg/ombdir15.html).

§170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

(a) Encryption and decryption of electronic health information
(1) General. Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2.
(2) Exchange. Any encrypted and integrity protected link.

(b) Record actions related to electronic health information. The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded.

(c) Verification that electronic health information has not been altered in transit.

Standard. A hashing algorithm with a security strength equal to or greater than SHA-1 (Secure Hash Algorithm (SHA-1)) as specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-3 (October, 2008)) must be used to verify that electronic health information has not been altered.

(d) Record treatment, payment, and health care operations disclosures.
The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.