NCHICA
North Carolina Healthcare Information and Communications Alliance, Inc.

Response to "Revisions to the Permanent Certification Program for Health Information Technology" NPRM (RIN 0991-AB82)

May 7, 2012

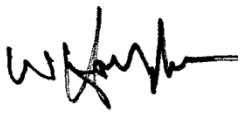
Secretary Kathleen Sebelius
U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Attention: 2014 Edition EHR Standards & Certification Criteria Proposed Rule
Hubert H. Humphrey Building, Suite 729D
200 Independence Avenue, SW, Washington, DC 20201

Dear Secretary Sebelius:

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) is a nationally-recognized nonprofit consortium that serves as an open, effective, and neutral forum for health information technology initiatives that improve health and care. NCHICA is comprised of over 230 member organizations representing the many sectors of the healthcare industry, including covered entities like providers and health plans, as well as government agencies, clearinghouses, business associates, research organizations, health care vendors, and attorneys.

NCHICA's comments on this Notice of Proposed Rulemaking (NPRM) are the result of a collaborative effort from NCHICA's various and diverse member organizations, which have considerable combined expertise in the various aspects of healthcare delivery, healthcare information technology, and the HIPAA regulations.

Respectfully submitted,



W. Holt Anderson
Executive Director

Office of the National Coordinator for Health IT
Proposed Rule Public Comment Template

Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology

Preface

This document is meant to provide the public with a simple and organized way to submit comments on the proposed certification criteria and associated standards and implementation specifications and respond to specific questions posed in the preamble of the proposed rule, which is published in the Federal Register at 77 FR 13832 (March 7, 2012). While use of this document is entirely voluntary, commenters may find it helpful to use the document in lieu of or in addition to unstructured comments on the certification criteria and associated standards and implementation specifications or to use it as an addendum to narrative cover pages.

This document alone is not intended to provide a full and complete opportunity to comment on all of the provisions of the proposed rule. Please keep in mind that it only reflects those proposals included in the proposed rule related to certification criteria and associated standards and implementation specifications. Additionally, while each of the comment tables below indicate whether specific comments on a proposal are solicited, we note that the specific questions are not explicitly included in the tables to keep the size of this document to a minimum and because the preamble serves as the context for the questions.

The proposed rule proposes new, revised, and unchanged certification criteria that would establish the technical capabilities and specify the related standards and implementation specifications that Certified EHR Technology (CEHRT) would need to include to, at a minimum, support the achievement of meaningful use (MU) by eligible professionals (EPs), eligible hospitals (EHs), and critical access hospitals (CAHs) under the CMS Medicare and Medicaid EHR Incentive Programs beginning with the EHR reporting periods in fiscal year (FY) for EHs and CAHs and calendar year (CY) 2014 for EPs. We refer to these new, revised, and unchanged certification criteria as the "2014 Edition EHR certification criteria."

Many of the certification criteria that we propose are intended to support the MU objectives and measures proposed in the CMS Medicare and Medicaid EHR Incentive Programs Stage 2 proposed rule (CMS Stage 2 proposed rule) (77 FR 13698) as well as the reporting of MU objectives and measures and clinical quality measures (CQMs) to CMS. To the extent CMS may change (e.g., add, revise, or remove) MU objectives, measures, or reporting requirements in a final rule, we may also find it necessary or appropriate to change proposed supporting certification criteria. Commenters recommending changes to the proposed MU objectives and measures, CQMs, or reporting requirements should consider whether changes to the certification criteria would also be needed and offer those suggested changes. Similarly, commenters should consider and specify whether any of their suggested revisions to the proposed certification criteria would impact the proposals in CMS's Stage 2 proposed rule.

The following tables align with the presentation of the proposed certification criteria in the preamble of the proposed rule. The tables specify where the proposed 2014 Edition EHR certification criterion or criteria would be included in § 170.314. The tables also specify the MU objective that the proposed 2014 Edition EHR certification criterion or criteria and associated standards and implementation specifications support. The objective cited is either a Stage 1 or Stage 2 objective that would be effective for the EHR reporting periods in FY/CY 2014. We provide this frame of reference because we propose that beginning in FY/CY 2014, EHR technology would need to be certified to the 2014 Edition EHR certification criteria to meet the definition of

CEHRT and the tables permit commenters to easily associate the certification criterion or criteria with the MU objective it supports. The tables note the page(s) of the Federal Register where we discuss the certification criterion or criteria and whether we request specific comments on certain proposals in the preamble. Last, the tables provide a field for submitting public comments on the proposed criterion or criteria, including responses to specific questions or requests for comments posed in the preamble.

To be considered, all comments (including comments provided through this document) must be submitted according to the instructions in the proposed rule, which are available at 77 FR 13832 (March 7, 2012).

Proposed 2014 Edition EHR Certification Criteria

New Certification Criteria

a. Ambulatory and Inpatient Setting

§ 170.314(e)(1) - View, download, and transmit to 3rd party

MU Objective

EPs

Provide patients the ability to view online, download, and transmit their health information within 4 business days of the information being available to the EP.

EHs and CAHs

Provide patients the ability to view online, download, and transmit information about a hospital admission.

2014 Edition EHR Certification Criterion

View, download, and transmit to 3rd party.

(i) Enable a user to provide patients (and their authorized representatives) with online access to do all of the following:

(A) View. Electronically view in accordance with the standard adopted at § 170.204(a), at a minimum, the following data elements:

(1) Patient name; gender; date of birth; race; ethnicity; preferred language; smoking status; problem list; medication list; medication allergy list; procedures; vital signs; laboratory tests and values/results; provider's name and contact information; names and contact information of any additional care team members beyond the referring or transitioning provider and the receiving provider; and care plan, including goals and instructions.

(2) Inpatient setting only. Admission and discharge dates and locations; reason(s) for hospitalization; names of providers of care during hospitalization; laboratory tests and values/results (available at time of discharge); and discharge instructions for patient.

(B) Download. Electronically download:

(1) A file in human readable format that includes, at a minimum:

(i) Ambulatory setting only. All of the data elements specified in paragraph (e)(1)(i)(A)(1).

(ii) Inpatient setting only. All of the data elements specified in paragraphs (e)(1)(i)(A)(1) and (e)(1)(i)(A)(2).

(2) A summary care record formatted according to the standards adopted at § 170.205(a)(3) and that includes, at a minimum, the following data elements expressed, where applicable, according to the specified standard(s):

(i) Patient name; gender; date of birth; medication allergies; vital signs; the provider's name and contact information; names and contact information of any additional care team members beyond the referring or transitioning provider and the receiving provider; care plan, including goals and instructions;

(ii) Race and ethnicity. The standard specified in § 170.207(f);

(iii) Preferred language. The standard specified in § 170.207(j);

(iv) Smoking status. The standard specified in § 170.207(l);

(v) Problems. At a minimum, the version of the standard specified in § 170.207(a)(3);

(vi) Encounter diagnoses. The standard specified in § 170.207(m);

(vii) Procedures. The standard specified in § 170.207(b)(2) or § 170.207(b)(3);

(viii) Laboratory test(s). At a minimum, the version of the standard specified in § 170.207(g);

(ix) Laboratory value(s)/result(s). The value(s)/results of the laboratory test(s) performed;

(x) Medications. At a minimum, the version of the standard specified in § 170.207(h); and

§ 170.314(e)(1) - View, download, and transmit to 3rd party

(xi) Inpatient setting only. The data elements specified in paragraph (e)(1)(i)(A)(2).

(3) Images formatted according to the standard adopted at § 170.205(j).

(C) Transmit to third party. Electronically transmit the summary care record created in paragraph (e)(1)(i)(B)(2) or images available to download in paragraph (e)(1)(i)(B)(3) in accordance with:

(1) The standard specified in § 170.202(a)(1); and

(2) The standard specified in § 170.202(a)(2).

(ii) Patient accessible log.

(A) When electronic health information is viewed, downloaded, or transmitted to a third-party using the capabilities included in paragraphs (e)(1)(i)(A)-(C), the following information must be recorded and made accessible to the patient:

(1) The electronic health information affected by the action(s);

(2) The date and time each action occurs in accordance with the standard specified at § 170.210(g);

(3) The action(s) that occurred; and

(4) User identification.

(B) EHR technology presented for certification may demonstrate compliance with paragraph (e)(1)(ii)(A) if it is also certified to the certification criterion adopted at § 170.314(d)(2) and the information required to be recorded in paragraph (e)(1)(ii)(A) is accessible by the patient.

Standard(s) and Implementation Specifications

§ 170.204(a) (Web Content Accessibility Guidelines (WCAG) 2.0, Level AA Conformance); § 170.205(a)(3) (Consolidated CDA); § 170.205(j) (DICOM PS 3—2011); § 170.207(f) (OMB standards for the classification of federal data on race and ethnicity); § 170.207(j) (ISO 639-1:2002 (preferred language)); § 170.207(l) (smoking status types); § 170.207(a)(3) (SNOMED-CT® International Release January 2012); § 170.207(m) (ICD-10-CM); § 170.207(b)(2) (HCPCS and CPT-4) or § 170.207(b)(3) (ICD-10-PCS); § 170.207(g) (LOINC version 2.38); § 170.207(h) (RxNorm February 6, 2012 Release); § 170.202(a)(1) (Applicability Statement for Secure Health Transport) and § 170.202(a)(2) (XDR and XDM for Direct Messaging); and § 170.210(g) (synchronized clocks).

Preamble FR Citation: 77 FR 13838-41	**Specific questions in preamble?** *Yes*

Public Comment Field:

With respect to the patient accessible log (170.314(e)(1)(ii)), we would like clarification on what is intended by the "electronic health information affected by the action." We are concerned this could be interpreted to mean granular auditing is required, for example, logging not only that a patient viewed their health information, but which health information elements were viewed. We do not support inclusion of specific PHI elements (such as a list of medications, lab results, etc.) in the audit trail. Storing this type of information may place a burden on providers to pay for extra storage space and may introduce performance problems. In addition, we question the value that this information adds to the patient's experience. Instead, we support auditing of the chart section or type of information viewed, transmitted, or downloaded. For example, the audit trail may contain an entry logging that a patient viewed their medication list, but does not log the specific medications that list contains.

In addition, we are concerned with the amount of information about clinical staff that will be available to patients, such as full name and contact information. Providing this information jeopardizes the privacy of healthcare workers and opens them up to potential harassment or harm, particularly in certain patient populations. For example, our members have indicated that full names of providers and staff are typically not available on name tags, directories, or in other locations in which certain patient populations, including mental health and emergency department patients, are treated. The risk of patients potentially harassing or causing harm to these providers and staff has been determined to be high enough risk to outweigh any benefit to patients in identifying the full names of employees. For the same reasons, many working with these populations have unlisted telephone numbers or other contact information. By making this information available to patients online, the NPRM removes these protections from individuals that provide these important services.

b. Ambulatory Setting

§ 170.314(e)(3) - Secure messaging

MU Objective

Use secure electronic messaging to communicate with patients on relevant health information.

§ 170.314(e)(3) - Secure messaging	
2014 Edition EHR Certification Criterion Ambulatory setting only – secure messaging. Enable a user to electronically send messages to, and receive messages from, a patient in a manner that ensures: (i) Both the patient and EHR technology are authenticated; and (ii) The message content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f). **Standard** § 170.210(f) Any encryption and hashing 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.	
Preamble FR Citation: 77 FR 13843-44	**Specific questions in preamble?** *No*
Public Comment Field: We agree with this criteria, and support its inclusion.	

c. Inpatient Setting

Revised Certification Criteria

a. Ambulatory and Inpatient Setting

§ 170.314(d)(2) - Auditable events and tamper-resistance; and (d)(3) - Audit report(s)
MU Objective Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.
2014 Edition EHR Certification Criteria (d)(2) Auditable events and tamper-resistance. (i) Enabled by default. The capability specified in paragraph (d)(2)(ii) must be enabled by default (i.e., turned on) and must only be permitted to be disabled (and re-enabled) by a limited set of identified users. (ii) Record actions. Record actions related to electronic health information and audit log status in accordance with the standard specified in § 170.210(e). (iii) Audit log protection. Actions recorded in accordance with paragraph (d)(3)(ii) must not be capable of being changed, overwritten, or deleted. (iv) Detection. Detect the alteration of audit logs. (d)(3) Audit report(s). Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the elements specified in the standard at § 170.210(e). **Standards** § 170.210(e) Record actions related to electronic health information, audit log status, and encryption of end-user devices. (1) When EHR technology is used to record, create, change, access, or delete electronic health information, the following information must be recorded: (i) The electronic health information affected by the action(s); (ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g);

§ 170.314(d)(2) - Auditable events and tamper-resistance; and (d)(3) - Audit report(s)	
(iii) The actions(s) that occurred; (iv) Patient identification; and (v) User identification. (2) When the audit log is enabled or disabled, the following must be recorded: (i) The date and time each action occurs in accordance with the standard specified at § 170.210(g); and (ii) User identification. (3) As applicable, when encryption of electronic health information managed by EHR technology on end-user devices is enabled or disabled, the following must be recorded: (i) The date and time in accordance with the standard specified at § 170.210(g); and (ii) User identification.	
Preamble FR Citation: 77 FR 13853-54	**Specific questions in preamble?** *No*

Public Comment Field:

We support audit logging being enabled by default. However, we would like to clarify that some EHRs do not provide the capability to disable the audit trail because of user base or technology choice. Therefore, we recommend updating the language in 170.314(d)(2)(i) to read (new text in italics) "...must be enabled by default and, *if the audit trail is able to be disabled*, must only be permitted to be disabled (and re-enabled) by a limited set of identified users." Likewise, we recommend that the language in 170.210(e)(2) be updated to read "*If the audit trail is able to be disabled*, when the audit trail is enabled or disabled, the following must be recorded..." In addition, when the audit log is stored outside the EHR, it is outside the scope of the EHR to audit actions that may disable, change, overwrite, or delete the audit log. For example, if the audit log is stored in a database, it is unreasonable to expect EHRs to audit actions performed against the database that may impact the audit trail (for instance, shutting the database down or modifying database tables).

We also seek clarity on the level of information that must be audited to satisfy 170.314(e)(1)(i). We are concerned that "electronic health information" may be interpreted to mean that PHI must be included in the audit trail. For example, if a user views a patient's medication list, we are concerned that this language may be interpreted that the medications that were viewed must be logged in the audit trail. Storing PHI in the audit trail violates separation of duties and the minimum necessary standard under HIPAA, since security auditors typically do not need this information to perform their duties. In addition, storing copies of PHI in the audit trail may lead to performance concerns and introduce undue burden on providers that must pay for the extra storage space to contain the logs. As such, we oppose storing PHI in the audit trail. We do, however, see value in logging the area or chart section that a user had access to. For example, if a user does not have a reason to access a patient's medications, logging that a user viewed the medication list (without the details of what specific medicines that list contained) is useful information for a security auditor to begin their investigation.

We recognize that storing a record of modifications made to a clinical record is important information to capture for clinicians, and recommend that ONC adopt a "Medical Record History & Completeness" objective that is separate from the security audit trail.

§ 170.314(d)(7) - Encryption of data at rest	
MU Objective Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	
2014 Edition EHR Certification Criterion Encryption of data at rest. Paragraph (d)(7)(i) or (d)(7)(ii) must be met to satisfy this certification criterion. (i) If EHR technology manages electronic health information on an end-user device and the electronic health information remains stored on the device after use of the EHR technology on that device has stopped, the electronic health information must be encrypted in accordance with the standard specified in § 170.210(a)(1). This capability must be enabled by default (i.e., turned on) and must only be permitted to be disabled (and re-enabled) by a limited set of identified users. (ii) Electronic health information managed by EHR technology never remains stored on end-user devices after use of the EHR technology on those devices has stopped.	
Preamble FR Citation: 77 FR 13854-55	**Specific questions in preamble?** *No*
Public Comment Field: We are supportive of this criteria, as lost laptops and other removable media count for the single largest source of breaches of unsecured PHI. However, we would like to make a few clarifications. First, we would like to clarify that this criteria is not requiring laptops, desktops, mobile devices, and other end user devices to be full-disk encrypted. The decision whether to deploy full-disk encryption should be based on an organization's HIPAA security risk assessment. Requiring full-disk encryption across the industry may be burdensome, especially on smaller practices that have other compensating controls in place. We would also like to clarify that when electronic health information is "managed" by the EHR. For example, if electronic health information is sent to a print queue, exported to a PDF in a report, or downloaded in a CCD, we view this information as no longer managed by the EHR. In addition, we point out that "end user device" is not defined in the text of the NPRM, and may lead to confusion in the market place if not defined. For example, in the commentary that accompanies the NPRM, USB flash drives are specifically called out of scope for end user device encryption. However, this is not called out in the text of the NPRM itself, possibly leading to confusion.	

b. Ambulatory Setting

No comments

c. Inpatient Setting

Unchanged Certification Criteria

a. Refinements to Unchanged Certification Criteria

§ 170.314(d)(1) - Authentication, access control, and authorization
MU Objective Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.
2014 Edition EHR Certification Criterion Authentication, access control, and authorization. (i) Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed; and (ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in

§ 170.314(d)(1) - Authentication, access control, and authorization

(d)(1)(i), and the actions the user is permitted to perform with the EHR technology.

Preamble FR Citation: 77 FR 13858-59	**Specific questions in preamble?** *No*

Public Comment Field:

We support the criteria remaining unchanged.

170.314(d)(5) - Automatic log-off

MU Objective

Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.

2014 Edition EHR Certification Criterion

Automatic log-off. Terminate an electronic session after a predetermined time of inactivity.

Preamble FR Citation: 77 FR 13859	**Specific questions in preamble?** *No*

Public Comment Field:

We support the criteria remaining unchanged.

§ 170.314(d)(6) - Emergency access

MU Objective

Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.

2014 Edition EHR Certification Criterion

Emergency access. Permit an identified set of users to access electronic health information during an emergency.

Preamble FR Citation: 77 FR 13859	**Specific questions in preamble?** *No*

Public Comment Field:

We support the criteria remaining unchanged.

§ 170.314(d)(8) – Integrity

MU Objective

Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.

2014 Edition EHR Certification Criterion

Integrity**.**

(i) Create a message digest in accordance with the standard specified in 170.210(c).

(iii) Verify in accordance with the standard specified in 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered.

§ 170.314(d)(8) – Integrity	
Standard § 170.210(c) (verification that electronic health information has not been altered)	
Preamble FR Citation: 77 FR 13859	**Specific questions in preamble?** *Yes*
Public Comment Field: We support the criteria remaining unchanged.	

b. Unchanged Certification Criteria Without Refinements

§ 170.314(d)(9) - Accounting of disclosures	
MU Objective Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	
2014 Edition EHR Certification Criterion Optional – accounting of disclosures. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in §170.210(d).	
Preamble FR Citation: 77 FR 13859, 13871-72	**Specific questions in preamble?** *Yes*
Public Comment Field: We support this criteria remaining optional.	