management systems in place without requiring them to rip and replace to conform to a ''standard'' quality management system that may not offer any significant improvement over what they already have in place. These commenters also stated that it is important for EHR technology developers who are currently following one of the existing ISO or FDA standard processes not be disadvantaged by new MU equivalencies.

Response. We appreciate the very thorough and thoughtful comments on our proposal to adopt a quality management system (QMS) oriented certification criterion. We share the sentiments expressed by commenters that selecting and implementing an optimal quality management system (QMS) for EHR technology development can be complex. We agree that existing standards may not explicitly state support for agile development methodologies and that such methods may be part of an optimal QMS. We appreciate the detailed comments that offered guidance regarding the optimal components of an ideal QMS for EHR technology and we agree with many of these suggestions. Because we were unable to publish the quality management document referenced in the Proposed Rule we recognize that there was an insufficient opportunity to comment on this document and have not included an explicit requirement to use this document.

We agree with the many commenters who described the advantages of an incremental implementation of QMS requirements for EHR technology. Additionally, we support the position of the commenters that stated this requirement should strive not to burden EHR technology developers with the task of documenting previous development processes. We disagree with the commenter who believed that this requirement was beyond our authority. The Secretary has the statutory authority to adopt standards, implementation specifications, and certification criteria for HIT and the National Coordinator has the statutory authority to establish a certification program for the certification of HIT to certification criteria adopted by the Secretary. Additionally, we disagree with the commenter with internally developed EHR technology that objected to our proposed gap analysis because we believe that the purchasers of EHR technology are not the only stakeholders who would take interest in the transparency provided by the submission of this information. Patients, employees, business partners, and shareholders of such organizations would be other such interested parties.

In consideration of comments received for and against this proposal, we have decided to adopt a certification criterion in this final rule at § 170.314(g)(4) that will generally focus on QMS and, as suggested by many commenters, is meant to be a first step that can be built on in an incremental fashion. All EHR technology certified to the 2014 Edition EHR certification criteria would need to be certified to this certification criterion, and we have taken steps to ensure that EHR Modules are certified to this certification criterion by revising § 170.550 as discussed in more detail under section IV.C.2 of this preamble.

We have adopted a certification criterion that accounts for the fact that we did not publish the quality management document as we had proposed. The certification criterion we have adopted is more general and provides more flexibility. The certification criterion expresses that for each capability an EHR technology includes and for which that capability's certification is sought, the use of a QMS in the development, testing, implementation and maintenance of that capability must be identified. Unlike our proposal, any QMS may be used to meet this certification criterion and even an indication that no QMS was used for particular capabilities for which certification is requested is permitted. The commenter who stated that they are implementing the FDA's Quality System (QS) regulations (for example, under the MDDS rule) would—by definition—be meeting this certification criterion so long as they cite their compliance with FDA's QS regulations for certification. Given this flexibility, we cannot foresee any reason why this certification criterion cannot be satisfied nor do we believe that it will be a significant burden to indicate the QMS used (or not used) in the development of capabilities for which certification is sought.

We understand that some EHR technology developers have several teams who work on different functional components of EHR technology. In the case where the whole development organization uses the same QMS (or not at all) across all teams, then this certification criterion may be met with one report. Where there is variability across teams, the EHR technology developer will need to indicate the individual QMS' followed for the applicable certification criteria for which the EHR technology is submitted for certification.

We encourage EHR technology developers to choose an established QMS, but developers are not required to do so, and may use either a modified version of an established QMS, or an entirely ''home grown'' QMS. We also clarify that we have no expectation that there will be detailed documentation of historical QMS or their absence. As specified above, we believe that the documentation of the current status of QMS in an EHR technology development organization is sufficient.

EHR Technology Safety Reporting

We also considered adopting a certification criterion (as mandatory or optional) that would require EHR technology to enable a user to generate a file in accordance with the data required by the Agency for Healthcare Research and Quality (AHRQ) Common Format,[15] including the ''Device or Medical/Surgical Supply, including HIT v1.1a.'' We requested public comment on whether we should adopt such a certification criterion and what, if any, challenges EHR technology developers would encounter in implementing this capability.

Comments. Many commenters requested that ONC not adopt a certification criterion at this time, but take the opportunity to study the role of EHRs in patient safety incident reporting in order to determine if something more reflective of EHR technology's role in such reporting as a future certification criterion would be appropriate. Many of these commenters also stated that there is insufficient experience with the AHRQ Common Format—especially in the ambulatory domain, and that extension of the Common Format would be necessary for it to be of value. Other commenters expressed additional concerns about the maturity of the Common Format, and the ability of EHR technology to generate the appropriate file format, and whether there would be any near-term value to such reports without more experience with adverse event reporting from EHR technology.

Response. We agree with these concerns and have not adopted a certification criterion for reporting patient safety events according to the Common Formats in the 2014 Edition EHR certification criteria.

- *Data Portability*

[15] *http://www.pso.ahrq.gov/formats/commonfmt.htm*

MU Objective N/A
2014 Edition EHR Certification Criterion
§ 170.314(b)(7) (Data portability).

In the Proposed Rule we sought public comment on whether we should adopt a certification criterion to focus on the portability of data stored within CEHRT. We recited the scenario where a provider might seek to change EHR technology (and EHR technology developers). We stated that in such a scenario providers should have the ability to easily switch EHR technology—at a low cost—and migrate most or all of their data in structured form to another EHR technology. We noted that in the absence of this capability, providers could be ''locked-in'' to their current EHR technology, which could ultimately impede innovation. With our belief that data portability is a key aspect of the EHR technology market that requires maturity, we sought public comment on specific questions that could inform our decision on whether to adopt a certification criterion focused on data portability. We asked: (1) Whether EHR technology is capable of electronically providing a sufficient amount of a patient's health history using export summaries formatted according to the Consolidated CDA for the scenario described above; (2) whether all of the data in a provider's EHR #1 is necessary to migrate over to EHR #2 in the event the provider wants to switch (We noted that potential effect of medical record retention laws, but sought to determine whether the loss of some data would be tolerable and if so, which data.); (3) considering the standards that have been adopted and proposed for adoption in the Proposed Rule, what additional standards and guidance would be necessary to meet market needs for data portability, including the portability of administrative data such as Medicare and Medicaid eligibility and claims; (4) whether a specific set of patient data could be used as a foundation for an incremental approach to improve data portability for the situation described above as well as other situations; and (5) whether the concept of a capability to batch export a single patient's records (or a provider's entire patient population) poses unintended consequences from a security perspective and what factors should be considered to mitigate any potential abuse of this capability if it existed.

Comments. Commenters strongly supported our efforts to improve data portability, including in the specific provider situation we outlined in the Proposed Rule. Many commenters generally noted that medical record retention laws, as well as those governing fraud and abuse investigations, largely determine the amount and type of information that must be retained, and therefore, needs to be portable. Commenters also noted that there may be other reasons for retaining longitudinal information on patient care, such as clinical trial participation, post approval study requirements and other clinical reasons.

Many commenters stated that some data loss is inevitable, with some commenters noting this was due to variations in clinical content and data schema(s) between EHR systems. Commenters gave varying responses on what specific data would be important to migrate to a new EHR. Some commenters stated the decision would be situational, best left to the provider, or, as previously noted, based on medical records retention laws and requirements. Commenters stated that demographics, problems, medications, medication allergies, allergies, immunizations, vital signs, lab results, and encounter notes would fall into the category of ''not tolerable'' to lose in transfer. For all ''other'' data, commenters stated that it would be sufficient for the data to be accessible in a human readable form through, but not necessarily stored within, the EHR. A few commenters also stated that documentation metadata should be readily available for all databases. Some commenters stated that the loss of data at a granular, visit-oriented level would be tolerable. Other commenters stated that because administrative data is normally stored in practice management systems—and not in EHRs—it would not need to be transferred from one of these systems to another.

One commenter suggested an incremental approach starting with requiring indexed and searchable documents including visit notes, letters, and reports. The commenter noted that this might require manual addition or automated generation of metadata and might need to include only documents generated after a given date for complete header information. The commenter noted that subsets of the patient's record (records of children must include immunizations and growth data) could be effective, but the commenter emphasized that the summary must be focused on the patient's lifetime data and not the most recent clinical events. Over time, the commenter stated that external standards for data portability would govern the internal structure of data within an EHR so that data can be exported and imported without data loss. The commenter stated that a good example is retention of laboratory results in LOINC® codes after import so that they can be exported in the future and used in a different EHR to identify data elements needed for clinical decision support or clinical quality measures.

Commenters stated that the Consolidated CDA would not be capable of sufficiently capturing all patient information that would be needed. Commenters stated that the Consolidated CDA is designed to be a summary and would not capture longitudinal patient information, administrative billing data, or other necessary data (e.g., trend analysis, operational data, and master file data). A few commenters noted that the CDA does not support the inclusion of information on whether meaningful use measures were applicable to or addressed for patients. Other commenters stated that CDA document types may not be the most efficient means to migrate data from one EHR to another. These commenters further stated that it is critical that such migration happens as quickly as possible. Therefore, the commenters contended that other data transfer mechanisms would be better suited for that purpose, particularly when large data volumes are in play (e.g., large multi-provider entities migrations).

A commenter stated that one possible solution would be to require EHR technology developers to tag key data elements that would typically be moved in an EHR transition with standardized XML. EHR technology developers would also need to be able to receive and process data feeds with this standardized XML, storing it in their native tables.

A few commenters stated that batch migrations are one of the more typical migration methods used when a provider moves from one EHR to another. Some commenters stated that batch exports of a patient's record poses serious security risks, while other commenters stated that current safeguards exist. These commenters pointed to the use of business associate agreements, encryption, and the use other internal controls to mitigate any security concerns.

Response. We thank commenters for the depth and breadth of their responses to our questions and proposals. In consideration of comments received, we have adopted a certification criterion for data portability. As discussed later in this final rule, we have also included this certification criterion as part of the Base EHR definition in order to ensure that all EPs, EHs, and CAHs, have this capability as part of the EHR technology they use to meet the CEHRT definition. While we recognize that no ‘‘silver bullet’’ exists with respect to data portability, we strongly believe that more attention must be paid to this market challenge and that with the interests of EPs, EHs, and CAHs in mind, small steps can be taken to improve the data portability between EHR technologies. We intend for this certification criterion to be a starting point and have framed it in such a way as to leverage capabilities that will already be included in an EP, EH, and CAH's CEHRT.

The certification criterion leverages and requires the same capabilities specified in the ‘‘transitions of care—create and transmit transition of care/referral summaries’’ certification criterion at § 170.314(b)(2)(i). The only difference between the capability specified in the data portability certification criterion and the capability specified in the transitions of care certification criterion is that the data portability certification criterion expressly limits the scope of the data to the most current clinical information about each patient for which an export summary is created. For the purposes of certification and for all of the patients on which an EP's, EH's, or CAH's CEHRT maintains data, the EHR technology must enable a user to electronically create a set of export summaries for all patients in EHR technology formatted according to the Consolidated CDA that includes each patient's most recent clinical information. While this is the minimum capability required for certification, we encourage EHR technology developers to include patients' longitudinal information for laboratory test results, immunizations, and procedures, and intend to consider including this broader requirement in the next edition of this certification criterion. We believe this initial capability provides a strong starting point for the fluid transition from one EHR technology to another. Primarily, we anticipate that this capability will be enable transitions to be more efficient by reducing the need for EPs, EHs, and CAHs to manually re-enter all of their patients' recent data into a new EHR system.

b. Ambulatory Setting

We propose to adopt 3 certification criteria that would be new certification criteria for the ambulatory setting.

- *Secure Messaging*

MU Objective
Use secure electronic messaging to communicate with patients on relevant health information.
2014 Edition EHR Certification Criterion
§ 170.314(e)(3) (Ambulatory setting only—secure messaging).

We proposed the 2014 Edition EHR certification criterion for secure messaging (at § 170.314(e)(3)) to support the MU objective and measure recommended by the HITPC and proposed by CMS. We agreed with the direction provided by both HITSC recommendations and merged the two into a refined proposed certification criterion. We also proposed to include in the certification criterion a baseline standard in terms of the encryption and hashing algorithms that would need to be used to implement secure messaging. More specifically, we proposed that only those identified in FIPS 140–2 Annex A be permitted to be used to meet this criterion and proposed to adopt a new standard in § 170.210(f) to refer to FIPS 140–2 Annex A's encryption and hashing algorithms. Additionally, we referenced several standards and implementations specifications that EHR technology developers could use to implement various secure messaging approaches, including IETF RFC 2246 (TLS 1.0), SMTP/SMIME, NIST Special Publication 800–52 (‘‘Guidelines for the Selection and Use of TLS Implementations''), and specifications developed as part of nationwide health information network initiatives.

Comments. Several commenters conveyed that the certification and testing process would need to accommodate the range of messaging mechanisms permitted by CMS, while being certified within the proposed standards. One commenter asked if there were approved modes of electronic messaging and whether secured and encrypted email would be a method. Another stated that use of a secure messaging capability from within a portal application should be an acceptable method. One commenter recommended that we equally support the standards and specifications developed as part of the NwHIN Exchange with the intent to support the broadest possible adoption of health information exchange capabilities. Other commenters generally requested that we provide some examples of common access mechanisms and acceptable security protocols. Another commenter suggested that we consider particular transport methods be certified similar to the certification criteria discussed in the Proposed Rule that referenced the Direct specifications and other acceptable transport methods. One commenter stressed the importance of adequate privacy and security, but urged ONC to take a reasonable approach and not make the use of secure electronic messaging to communicate with patients unduly burdensome. One commenter stated that functionality such as a patient portal would be handled through normal browser HTTPS functionality and, therefore, should be easily managed through a visual inspection and should not require additional verification. One commenter supported secure messaging in general, but did not support secure email as the only secure messaging methodology. The commenter indicated that they currently send patients an unsecure email prompt that they have a message and that upon receipt the patient can securely log-in to their patient portal using an SSL-protected session to retrieve the message and send new ones.

Response. We share commenters' sentiment that this certification criterion needs to permit/accommodate a range of possible innovative options. To that end, we intentionally proposed this certification criterion to only specify the particular baseline security and functional capabilities we believed were necessary to require for certification. So long as the method included with EHR technology presented for certification can meet these baseline requirements it would be able to meet this certification criterion. Thus, secure email, a secure portal, even some type of mobile application could all be examples for secure messaging methods that could potentially meet this certification criterion. Along those lines, we decline to specify or restrict certification in this case to a particular transport standard because, again, we intend to permit a wide range of different secure messaging solutions, that will likely use different approaches and transport standards.

In consideration of these comments and the ones responded to below, we are finalizing this certification criterion as proposed with one exception. The only modification we have made is to explicitly note as we already have in the view, download, and transmit to a 3rd party certification criterion that it could be the patient or their authorized representative that engages in secure messaging.

Comment. A commenter stated that patients must be able to directly communicate with health professionals via patient portals and OAuth.

Response. We decline to incorporate this suggestion into the certification criterion because it would be information for electronic transmission in accordance with:

(i) The standard specified in § 170.205(b)(2); and

(ii) At a minimum, the version of the standard specified in § 170.207(d)(2).

(4) *Clinical information reconciliation.* Enable a user to electronically reconcile the data that represent a patient's active medication, problem, and medication allergy list as follows. For each list type:

(i) Electronically and simultaneously display (i.e., in a single view) the data from at least two list sources in a manner that allows a user to view the data and their attributes, which must include, at a minimum, the source and last modification date.

(ii) Enable a user to create a single reconciled list of medications, medication allergies, or problems.

(iii) Enable a user to review and validate the accuracy of a final set of data and, upon a user's confirmation, automatically update the list.

(5) *Incorporate laboratory tests and values/results.* (i) *Receive results.* (A) *Ambulatory setting only.* (*1*) Electronically receive and incorporate clinical laboratory tests and values/results in accordance with the standard specified in § 170.205(j) and, at a minimum, the version of the standard specified in § 170.207(c)(2).

(*2*) Electronically display the tests and values/results received in human readable format.

(B) *Inpatient setting only.* Electronically receive clinical laboratory tests and values/results in a structured format and electronically display such tests and values/results in human readable format.

(ii) Electronically display all the information for a test report specified at 42 CFR 493.1291(c)(1) through (7).

(iii) Electronically attribute, associate, or link a laboratory test and value/result with a laboratory order or patient record.

(6) *Inpatient setting only—transmission of electronic laboratory tests and values/results to ambulatory providers.* EHR technology must be able to electronically create laboratory test reports for electronic transmission in accordance with the standard specified in § 170.205(j) and with laboratory tests expressed in accordance with, at a minimum, the version of the standard specified in § 170.207(c)(2).

(7) *Data portability.* Enable a user to electronically create a set of export summaries for all patients in EHR technology formatted according to the standard adopted at § 170.205(a)(3) that represents the most current clinical information about each patient and includes, at a minimum, the Common MU Data Set and the following data expressed, where applicable, according to the specified standard(s):

(i) *Encounter diagnoses.* The standard specified in § 170.207(i) or, at a minimum, the version of the standard at § 170.207(a)(3);

(ii) *Immunizations.* The standard specified in § 170.207(e)(2);

(iii) Cognitive status;

(iv) Functional status; and

(v) *Ambulatory setting only.* The reason for referral; and referring or transitioning provider's name and office contact information.

(vi) *Inpatient setting only.* Discharge instructions.

(c) Clinical quality measures. (1) *Clinical Quality Measures—capture and export.* (i) *Capture.* For each and every CQM for which the EHR technology is presented for certification, EHR technology must be able to electronically record all of the data identified in the standard specified at § 170.204(c) that would be necessary to calculate each CQM. Data required for CQM exclusions or exceptions must be codified entries, which may include specific terms as defined by each CQM, or may include codified expressions of ‘‘patient reason,'' ‘‘system reason,'' or ‘‘medical reason.''

(ii) *Export.* EHR technology must be able to electronically export a data file formatted in accordance with the standards specified at § 170.205(h) that includes all of the data captured for each and every CQM to which EHR technology was certified under paragraph (c)(1)(i) of this section.

(2) *Clinical quality measures—import and calculate.* (i) *Import.* EHR technology must be able to electronically import a data file formatted in accordance with the standard specified at § 170.205(h) and use such data to perform the capability specified in paragraph (c)(2)(ii) of this section. EHR technology presented for certification to all three of the certification criteria adopted in paragraphs (c)(1) through (3) of this section is not required to meet paragraph (c)(2)(i).

(ii) *Calculate.* EHR technology must be able to electronically calculate each and every clinical quality measure for which it is presented for certification.

(3) *Clinical quality measures—electronic submission.* Enable a user to electronically create a data file for transmission of clinical quality measurement data:

(i) In accordance with the standards specified at § 170.205(h) and (k); and

(ii) That can be electronically accepted by CMS.

(d) Privacy and security. (1) *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 paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the EHR technology.

(2) *Auditable events and tamper-resistance.* (i) *Record actions.* EHR technology must be able to:

(A) Record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1);

(B) Record the audit log status (enabled or disabled) in accordance with the standard specified in § 170.210(e)(2) unless it cannot be disabled by any user; and

(C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by EHR technology in accordance with the standard specified in § 170.210(e)(3) unless the EHR technology prevents electronic health information from being locally stored on end-user devices (see 170.314(d)(7) of this section).

(ii) *Default setting.* EHR technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) or (C), or both paragraphs (d)(2)(i)(B) and (C).

(iii) *When disabling the audit log is permitted.* For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that EHR technology permits to be disabled, the ability to do so must be restricted to a limited set of identified users.

(iv) *Audit log protection.* Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the EHR technology.

(v) *Detection.* EHR technology must be able to detect whether the audit log has been altered.

(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 data specified in the standards at § 170.210(e).

(4) *Amendments.* Enable a user to electronically select the record affected by a patient's request for amendment and perform the capabilities specified in paragraphs (d)(4)(i) or (ii) of this section.