20894; Telephone (301) 594–5983 or *http://www.nlm.nih.gov/*.

(1) International Health Terminology Standards Development Organization Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®), International Release, July 2009, IBR approved for § 170.207.

(2) International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®) International Release July 31, 2012, IBR approved for § 170.207.

(3) US Extension to SNOMED CT® March 2012 Release, IBR approved for § 170.207.

(4)–(5) [Reserved]

(6) International Health Terminology Standards Development Organization (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®) U.S. Edition, September 2015 Release, IBR approved for § 170.207(a).

(7) RxNorm, September 8, 2015 Full Release Update, IBR approved for § 170.207(d).

(s) World Wide Web Consortium (W3C)/MIT, 32 Vassar Street, Room 32–G515, Cambridge, MA 02139 USA, *http://www.w3.org/standards/*

(1) Web Content Accessibility Guidelines (WCAG) 2.0, December 11, 2008, IBR approved for § 170.204.

(2) [Reserved]

[75 FR 44649, July 28, 2010, as amended at 75 FR 62690, Oct. 13, 2010; 77 FR 54285, Sept. 4, 2012; 77 FR 72991, Dec. 7, 2012; 79 FR 54478, Sept. 11, 2014; 80 FR 62745, Oct. 16, 2015; 81 FR 72463, Oct. 19, 2016; 85 FR 25941, May 1, 2020; 85 FR 70082, Nov. 4, 2020]

Subpart C—Certification Criteria for Health Information Technology

SOURCE: 75 FR 44651, July 28, 2010, unless otherwise noted.

§ 170.300 Applicability.

(a) The certification criteria adopted in this subpart apply to the testing and certification of Health IT Modules.

(b) When a certification criterion refers to two or more standards as alternatives, use of at least one of the alternative standards will be considered compliant.

(c) Health Modules are not required to be compliant with certification criteria or capabilities specified within a certification criterion that are designated as optional.

(d) In § 170.315, all certification criteria and all capabilities specified within a certification criterion have general applicability (*i.e.*, apply to any health care setting) unless designated as ''inpatient setting only'' or ''ambulatory setting only.''

[75 FR 44649, July 28, 2010, as amended at 77 FR 54286, Sept. 4, 2012; 80 FR 62747, Oct. 16, 2015; 85 FR 25941, May 1, 2020; 85 FR 70083, Nov. 4, 2020]

§§ 170.302–170.306 [Reserved]

§ 170.314 [Reserved]

§ 170.315 2015 Edition health IT certification criteria.

The Secretary adopts the following certification criteria for health IT. Health IT must be able to electronically perform the following capabilities in accordance with all applicable standards and implementation specifications adopted in this part:

(a) *Clinical*—(1) *Computerized provider order entry—medications.* (i) Enable a user to record, change, and access medication orders.

(ii) *Optional.* Include a ''reason for order'' field.

(2) *Computerized provider order entry—laboratory.* (i) Enable a user to record, change, and access laboratory orders.

(ii) *Optional.* Include a ''reason for order'' field.

(3) *Computerized provider order entry—diagnostic imaging.* (i) Enable a user to record, change, and access diagnostic imaging orders.

(ii) *Optional.* Include a ''reason for order'' field.

(4) *Drug-drug, drug-allergy interaction checks for CPOE*—(i) *Interventions.* Before a medication order is completed and acted upon during computerized provider order entry (CPOE), interventions must automatically indicate to a user drug-drug and drug-allergy contraindications based on a patient's medication list and medication allergy list.

(ii) *Adjustments.* (A) Enable the severity level of interventions provided for drug-drug interaction checks to be adjusted.

(B) Limit the ability to adjust severity levels in at least one of these two ways:

(*1*) To a specific set of identified users.

(*2*) As a system administrative function.

(5)*Demographics*. (i) Enable a user to record, change, and access patient demographic data including race, ethnicity, preferred language, sex, sexual orientation, gender identity, and date of birth.

(A) *Race and ethnicity*. (*1*) Enable each one of a patient's races to be recorded in accordance with, at a minimum, the standard specified in §170.207(f)(2) and whether a patient declines to specify race.

(*2*) Enable each one of a patient's ethnicities to be recorded in accordance with, at a minimum, the standard specified in §170.207(f)(2) and whether a patient declines to specify ethnicity.

(*3*) Aggregate each one of the patient's races and ethnicities recorded in accordance with paragraphs (a)(5)(i)(A)(*1*) and (*2*) of this section to the categories in the standard specified in §170.207(f)(1).

(B) *Preferred language*. Enable preferred language to be recorded in accordance with the standard specified in §170.207(g)(2) and whether a patient declines to specify a preferred language.

(C) *Sex*. Enable sex to be recorded in accordance with the standard specified in §170.207(n)(1).

(D) *Sexual orientation*. Enable sexual orientation to be recorded in accordance with the standard specified in §170.207(o)(1) and whether a patient declines to specify sexual orientation.

(E) *Gender identity*. Enable gender identity to be recorded in accordance with the standard specified in §170.207(o)(2) and whether a patient declines to specify gender identity.

(ii) *Inpatient setting only*. Enable a user to record, change, and access the preliminary cause of death and date of death in the event of mortality.

(6)–(8) [Reserved]

(9) *Clinical decision support (CDS)*—(i) *CDS intervention interaction*. Interventions provided to a user must occur when a user is interacting with technology.

(ii) *CDS configuration*. (A) Enable interventions and reference resources specified in paragraphs (a)(9)(iii) and (iv) of this section to be configured by a limited set of identified users (*e.g.*, system administrator) based on a user's role.

(B) Enable interventions:

(*1*) Based on the following data:

(*i*) Problem list;

(*ii*) Medication list;

(*iii*) Allergy and intolerance list;

(*iv*) At least one demographic specified in paragraph (a)(5)(i) of this section;

(*v*) Laboratory tests; and

(*vi*) Vital signs.

(*2*) When a patient's medications, allergies and intolerance, and problems are incorporated from a transition of care/referral summary received and pursuant to paragraph (b)(2)(iii)(D) of this section.

(iii) *Evidence-based decision support interventions*. Enable a limited set of identified users to select (*i.e.*, activate) electronic CDS interventions (in addition to drug-drug and drug-allergy contraindication checking) based on each one and at least one combination of the data referenced in paragraphs (a)(9)(ii)(B)(*1*)(*i*) through (*vi*) of this section.

(iv) *Linked referential CDS*. (A) Identify for a user diagnostic and therapeutic reference information in accordance at least one of the following standards and implementation specifications:

(*1*) The standard and implementation specifications specified in §170.204(b)(3).

(*2*) The standard and implementation specifications specified in §170.204(b)(4).

(B) For paragraph (a)(9)(iv)(A) of this section, technology must be able to identify for a user diagnostic or therapeutic reference information based on each one and at least one combination of the data referenced in paragraphs (a)(9)(ii)(B)(*1*)(*i*), (*ii*), and (*iv*) of this section.

(v) *Source attributes*. Enable a user to review the attributes as indicated for all CDS resources:

(A) For evidence-based decision support interventions under paragraph (a)(9)(iii) of this section:

(*1*) Bibliographic citation of the intervention (clinical research/guideline);

(*2*) Developer of the intervention (translation from clinical research/guideline);

(*3*) Funding source of the intervention development technical implementation; and

(*4*) Release and, if applicable, revision date(s) of the intervention or reference source.

(B) For linked referential CDS in paragraph (a)(9)(iv) of this section and drug-drug, drug-allergy interaction checks in paragraph (a)(4) of this section, the developer of the intervention, and where clinically indicated, the bibliographic citation of the intervention (clinical research/guideline).

(10) *Drug-formulary and preferred drug list checks.* The requirements specified in one of the following paragraphs (that is, paragraphs (a)(10)(i) and (a)(10)(ii) of this section) must be met to satisfy this certification criterion:

(i) *Drug formulary checks.* Automatically check whether a drug formulary exists for a given patient and medication.

(ii) *Preferred drug list checks.* Automatically check whether a preferred drug list exists for a given patient and medication.

(11) [Reserved]

(12) *Family health history.* Enable a user to record, change, and access a patient's family health history in accordance with the familial concepts or expressions included in, at a minimum, the version of the standard in § 170.207(a)(4).

(13) *Patient-specific education resources.* (i) Identify patient-specific education resources based on data included in the patient's problem list and medication list in accordance with at least one of the following standards and implementation specifications:

(A) The standard and implementation specifications specified in § 170.204(b)(3).

(B) The standard and implementation specifications specified in § 170.204(b)(4).

(ii) *Optional.* Request that patient-specific education resources be identified in accordance with the standard in § 170.207(g)(2).

(14) *Implantable device list.* (i) Record Unique Device Identifiers associated with a patient's Implantable Devices.

(ii) Parse the following identifiers from a Unique Device Identifier:

(A) Device Identifier; and

(B) The following identifiers that compose the Production Identifier:

(*1*) The lot or batch within which a device was manufactured;

(*2*) The serial number of a specific device;

(*3*) The expiration date of a specific device;

(*4*) The date a specific device was manufactured; and

(*5*) For an HCT/P regulated as a device, the distinct identification code required by 21 CFR 1271.290(c).

(iii) Obtain and associate with each Unique Device Identifier:

(A) A description of the implantable device referenced by at least one of the following:

(*1*) The ''GMDN PT Name'' attribute associated with the Device Identifier in the Global Unique Device Identification Database.

(*2*) The ''SNOMED CT® Description'' mapped to the attribute referenced in in paragraph (a)(14)(iii)(A)(*1*) of this section.

(B) The following Global Unique Device Identification Database attributes:

(*1*) ''Brand Name'';

(*2*) ''Version or Model'';

(*3*) ''Company Name'';

(*4*) ''What MRI safety information does the labeling contain?''; and

(*5*) ''Device required to be labeled as containing natural rubber latex or dry natural rubber (21 CFR 801.437).''

(iv) Display to a user an implantable device list consisting of:

(A) The active Unique Device Identifiers recorded for the patient;

(B) For each active Unique Device Identifier recorded for a patient, the description of the implantable device specified by paragraph (a)(14)(iii)(A) of this section; and

(C) A method to access all Unique Device Identifiers recorded for a patient.

(v) For each Unique Device Identifier recorded for a patient, enable a user to access:

(A) The Unique Device Identifier;

(B) The description of the implantable device specified by paragraph (a)(14)(iii)(A) of this section;

(C) The identifiers associated with the Unique Device Identifier, as specified by paragraph (a)(14)(ii) of this section; and

(D) The attributes associated with the Unique Device Identifier, as specified by paragraph (a)(14)(iii)(B) of this section.

(vi) Enable a user to change the status of a Unique Device Identifier recorded for a patient.

(15) *Social, psychological, and behavioral data.* Enable a user to record, change, and access the following patient social, psychological, and behavioral data:

(i) *Financial resource strain.* Enable financial resource strain to be recorded in accordance with the standard specified in §170.207(p)(1) and whether a patient declines to specify financial resource strain.

(ii) *Education.* Enable education to be recorded in accordance with the standard specified in §170.207(p)(2) and whether a patient declines to specify education.

(iii) *Stress.* Enable stress to be recorded in accordance with the standard specified in §170.207(p)(3) and whether a patient declines to specify stress.

(iv) *Depression.* Enable depression to be recorded in accordance with the standard specified in §170.207(p)(4) and whether a patient declines to specify depression.

(v) *Physical activity.* Enable physical activity to be recorded in accordance with the standard specified in §170.207(p)(5) and whether a patient declines to specify physical activity.

(vi) *Alcohol use.* Enable alcohol use to be recorded in accordance with the standard specified in §170.207(p)(6) and whether a patient declines to specify alcohol use.

(vii) *Social connection and isolation.* Enable social connection and isolation to be recorded in accordance the standard specified in §170.207(p)(7) and whether a patient declines to specify social connection and isolation.

(viii) *Exposure to violence (intimate partner violence).* Enable exposure to violence (intimate partner violence) to be recorded in accordance with the standard specified in §170.207(p)(8) and whether a patient declines to specify exposure to violence (intimate partner violence).

(b) *Care coordination*—(1) *Transitions of care*—(i) *Send and receive via edge protocol.* (A) Send transition of care/referral summaries through a method that conforms to the standard specified in §170.202(d) and that leads to such summaries being processed by a service that has implemented the standard specified in §170.202(a)(2); and

(B) Receive transition of care/referral summaries through a method that conforms to the standard specified in §170.202(d) from a service that has implemented the standard specified in §170.202(a)(2).

(C) *XDM processing.* Receive and make available the contents of a XDM package formatted in accordance with the standard adopted in §170.205(p)(1) when the technology is also being certified using an SMTP-based edge protocol.

(ii) *Validate and display*—(A) *Validate C–CDA conformance—system performance.* Demonstrate the ability to detect valid and invalid transition of care/referral summaries received and formatted in accordance with the standards specified in §170.205(a)(3), (4), and (5) for the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates. This includes the ability to:

(*1*) Parse each of the document types.

(*2*) Detect errors in corresponding ''document-templates,'' ''section-templates,'' and ''entry-templates,'' including invalid vocabulary standards and codes not specified in the standards adopted in §170.205(a)(3), (4), and (5).

(*3*) Identify valid document-templates and process the data elements required in the corresponding section-templates and entry-templates from the standards adopted in §170.205(a)(3), (4), and (5).

(*4*) Correctly interpret empty sections and null combinations.

(*5*) Record errors encountered and allow a user through at least one of the following ways to:

(*i*) Be notified of the errors produced.

(*ii*) Review the errors produced.

(B) *Display*. Display in human readable format the data included in transition of care/referral summaries received and formatted according to the standards specified in §170.205(a)(3), (4), and (5).

(C) *Display section views*. Allow for the individual display of each section (and the accompanying document header information) that is included in a transition of care/referral summary received and formatted in accordance with the standards adopted in §170.205(a)(3), (4), and (5) in a manner that enables the user to:

(*1*) Directly display only the data within a particular section;

(*2*) Set a preference for the display order of specific sections; and

(*3*) Set the initial quantity of sections to be displayed.

(iii) *Create*. Enable a user to create a transition of care/referral summary formatted in accordance with the standard specified in §170.205(a)(3), (4), and (5) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates that includes, at a minimum:

(A)(*1*) The data classes expressed in the standard in §170.213 and in accordance with §170.205(a)(4), (5), and paragraphs (b)(1)(iii)(A)(*3*)(*i*) through (*iii*) of this section, or

(*2*) The Common Clinical Data Set in accordance with §170.205(a)(4) and paragraph (b)(1)(iii)(A)(*3*)(*i*) through (*iv*) of this section for the period before December 31, 2022, and

(*3*) The following data classes:

(*i*) *Assessment and plan of treatment*. In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in §170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in §170.205(a)(4).

(*ii*) *Goals*. In accordance with the ''Goals Section'' of the standard specified in §170.205(a)(4).

(*iii*) *Health concerns*. In accordance with the ''Health Concerns Section'' of the standard specified in §170.205(a)(4).

(*iv*) *Unique device identifier(s) for a patient's implantable device(s)*. In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in §170.205(a)(4).

(B) *Encounter diagnoses*. Formatted according to at least one of the following standards:

(*1*) The standard specified in §170.207(i).

(*2*) At a minimum, the version of the standard specified in §170.207(a)(4).

(C) Cognitive status.

(D) Functional status.

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

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

(G) *Patient matching data*. First name, last name, previous name, middle name (including middle initial), suffix, date of birth, address, phone number, and sex. The following constraints apply:

(*1*) *Date of birth constraint*. (*i*) The year, month and day of birth must be present for a date of birth. The technology must include a null value when the date of birth is unknown.

(*ii*) *Optional*. When the hour, minute, and second are associated with a date of birth the technology must demonstrate that the correct time zone offset is included.

(*2*) *Phone number constraint*. Represent phone number (home, business, cell) in accordance with the standards adopted in §170.207(q)(1). All phone numbers must be included when multiple phone numbers are present.

(*3*) *Sex constraint*. Represent sex in accordance with the standard adopted in §170.207(n)(1).

(2) *Clinical information reconciliation and incorporation*—(i) *General requirements*. Paragraphs (b)(2)(ii) and (iii) of this section must be completed based on the receipt of a transition of care/referral summary formatted in accordance with the standards adopted in §170.205(a)(3) through (5) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates on and after December 31, 2022.

(ii) *Correct patient*. Upon receipt of a transition of care/referral summary formatted according to the standards adopted §170.205(a)(3) through (5), technology must be able to demonstrate that the transition of care/referral

summary received can be properly matched to the correct patient.

(iii) *Reconciliation.* Enable a user to reconcile the data that represent a patient's active medication list, allergies and intolerance list, and problem list as follows. For each list type:

(A) Simultaneously display (*i.e.*, in a single view) the data from at least two 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.

(B) Enable a user to create a single reconciled list of each of the following: Medications; Allergies and Intolerances; and problems.

(C) Enable a user to review and validate the accuracy of a final set of data.

(D) Upon a user's confirmation, automatically update the list, and incorporate the following data expressed according to the specified standard(s) on and after December 31, 2022:

(*1*) *Medications.* At a minimum, the version of the standard specified in §170.213;

(*2*) *Allergies and intolerance.* At a minimum, the version of the standard specified in §170.213; and

(*3*) *Problems.* At a minimum, the version of the standard specified in §170.213.

(iv) *System verification.* Based on the data reconciled and incorporated, the technology must be able to create a file formatted according to the standard specified in §170.205(a)(4) using the Continuity of Care Document template and the standard specified in §170.205(a)(5) on and after December 31, 2022.

(3) *Electronic prescribing.* (i) For technology certified prior to June 30, 2020, subject to the real world testing provisions at §170.405(b)(5),

(A) Enable a user to perform the following prescription-related electronic transactions in accordance with, at a minimum, the version of the standard specified in §170.207(d)(3) as follows:

(*1*) Create new prescriptions (NEWRX).

(*2*) Change prescriptions (RXCHG, CHGRES).

(*3*) Cancel prescriptions (CANRX, CANRES).

(*4*) Refill prescriptions (REFREQ, REFRES).

(*5*) Receive fill status notifications (RXFILL).

(*6*) Request and receive medication history information (RXHREQ, RXHRES).

(B) For each transaction listed in paragraph (b)(3)(i)(A) of this section, the technology must be able to receive and transmit the reason for the prescription using the diagnosis elements in the DRU Segment.

(C) *Optional:* For each transaction listed in paragraph (b)(3)(i)(A) of this section, the technology must be able to receive and transmit the reason for prescription using the indication elements in the SIG Segment.

(D) Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (*i.e.*, not cc).

(E) Always insert leading zeroes before the decimal point for amounts less than one and must not allow trailing zeroes after a decimal point when a user prescribes medications.

(ii) For technology certified subsequent to June 30, 2020:

(A) Enable a user to perform the following prescription-related electronic transactions in accordance with the standard specified in §170.205(b)(1) and, at a minimum, the version of the standard specified in §170.207(d)(3) as follows:

(*1*) Create new prescriptions (NewRx).

(*2*) Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse).

(*3*) Request and respond to cancel prescriptions (CancelRx, CancelRxResponse).

(*4*) Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse).

(*5*) Receive fill status notifications (RxFill).

(*6*) Request and receive medication history (RxHistoryRequest, RxHistoryResponse).

(*7*) Relay acceptance of a transaction back to the sender (Status).

(*8*) Respond that there was a problem with the transaction (Error).

(*9*) Respond that a transaction requesting a return receipt has been received (Verify).

(B) Optionally, enable a user to perform the following prescription-related electronic transactions in accordance

with the standard specified in §170.205(b)(1) and, at a minimum, the version of the standard specified in §170.207(d)(3) as follows:

(*1*) Create and respond to new prescriptions (NewRxRequest, NewRxResponseDenied).

(*2*) Send fill status notifications (RxFillIndicatorChange).

(*3*) Ask the Mailbox if there are any transactions (GetMessage).

(*4*) Request to send an additional supply of medication (Resupply).

(*5*) Communicate drug administration events (DrugAdministration).

(*6*) Request and respond to transfer one or more prescriptions between pharmacies (RxTransferRequest, RxTransferResponse, RxTransferConfirm).

(*7*) Recertify the continued administration of a medication order (Recertification).

(*8*) Complete Risk Evaluation and Mitigation Strategy (REMS) transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse).

(*9*) Electronic prior authorization transactions (PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse).

(C) For the following prescription-related transactions, the technology must be able to receive and transmit the reason for prescription using the diagnosis elements: <Diagnosis> <Primary> or <Secondary>:

(*1*) *Required transactions:*

(*i*) Create new prescriptions (NewRx).

(*ii*) Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse).

(*iii*) Cancel prescriptions (CancelRx).

(*iv*) Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse).

(*v*) Receive fill status notifications (RxFill).

(*vi*) Receive medication history (RxHistoryResponse).

(*2*) *Optional transactions:*

(*i*) Request to send an additional supply of medication (Resupply)

(*ii*) Request and respond to transfer one or more prescriptions between pharmacies (RxTransferRequest, RxTransferResponse)

(*iii*) Complete Risk Evaluation and Mitigation Strategy (REMS) transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse).

(*iv*) Electronic prior authorization (ePA) transactions (PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse and PACancelRequest, PACancelResponse).

(D) *Optional:* For each transaction listed in paragraph (b)(3)(ii)(C) of this section, the technology must be able to receive and transmit reason for prescription using the <IndicationforUse> element in the SIG segment.

(E) Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (*i.e.*, not cc).

(F) Always insert leading zeroes before the decimal point for amounts less than one and must not allow trailing zeroes after a decimal point when a user prescribes medications.

(4)–(5) [Reserved]

(6) *Data export*—(i) *General requirements for export summary configuration*. (A) Enable a user to set the configuration options specified in paragraphs (b)(6)(iii) and (iv) of this section when creating an export summary as well as a set of export summaries for patients whose information is stored in the technology. A user must be able to execute these capabilities at any time the user chooses and without subsequent developer assistance to operate.

(B) Limit the ability of users who can create export summaries in at least one of these two ways:

(*1*) To a specific set of identified users.

(*2*) As a system administrative function.

(ii) *Creation*. Enable a user to create export summaries formatted in accordance with the standard specified in §170.205(a)(4) using the Continuity of Care Document document template that includes, at a minimum:

(A) The Common Clinical Data Set.

(B) *Encounter diagnoses*. Formatted according to at least one of the following standards:

(*1*) The standard specified in §170.207(i).

(*2*) At a minimum, the version of the standard specified in §170.207(a)(4).

(C) Cognitive status.

(D) Functional status.

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

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

(iii) *Timeframe configuration*. (A) Enable a user to set the date and time period within which data would be used to create the export summaries. This must include the ability to enter in a start and end date and time range.

(B) Consistent with the date and time period specified in paragraph (b)(6)(iii)(A) of this section, enable a user to do each of the following:

(*1*) Create export summaries in real-time;

(*2*) Create export summaries based on a relative date and time (*e.g.*, the first of every month at 1:00 a.m.); and

(*3*) Create export summaries based on a specific date and time (*e.g.*, on 10/24/2015 at 1:00 a.m.).

(iv) *Location configuration*. Enable a user to set the storage location to which the export summary or export summaries are intended to be saved.

(7) *Security tags—summary of care—send*. Enable a user to create a summary record formatted in accordance with the standard adopted in §170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in §170.205(o)(1) at the:

(i) Document, section, and entry (data element) level; or

(ii) Document level for the period before December 31, 2022.

(8) *Security tags—summary of care—receive*. (i) Enable a user to receive a summary record that is formatted in accordance with the standard adopted in §170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in §170.205(o)(1) at the:

(A) Document, section, and entry (data element) level; or

(B) Document level for the period before December 31, 2022; and

(ii) Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

(9) *Care plan*. Enable a user to record, change, access, create, and receive care plan information in accordance with:

(i) The Care Plan document template, including the Health Status Evaluations and Outcomes Section and Interventions Section (V2), in the standard specified in §170.205(a)(4); and

(ii) The standard in §170.205(a)(5) on and after December 31, 2022.

(10) *Electronic Health Information export*—(i) *Single patient electronic health information export*. (A) Enable a user to timely create an export file(s) with all of a single patient's electronic health information that can be stored at the time of certification by the product, of which the Health IT Module is a part.

(B) A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(C) Limit the ability of users who can create export file(s) in at least one of these two ways:

(*1*) To a specific set of identified users

(*2*) As a system administrative function.

(D) The export file(s) created must be electronic and in a computable format.

(E) The publicly accessible hyperlink of the export's format must be included with the exported file(s).

(ii) *Patient population electronic health information export*. Create an export of all the electronic health information that can be stored at the time of certification by the product, of which the Health IT Module is a part.

(A) The export created must be electronic and in a computable format.

(B) The publicly accessible hyperlink of the export's format must be included with the exported file(s).

(iii) *Documentation*. The export format(s) used to support paragraphs (b)(10)(i) and (ii) of this section must be kept up-to-date.

(c) *Clinical quality measures*—(1) *Clinical quality measures—record and export*—(i) *Record*. For each and every CQM for which the technology is presented for certification, the technology must be able to record all of the data

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.* A user must be able to export a data file at any time the user chooses and without subsequent developer assistance to operate:

(A) Formatted in accordance with the standard specified in §170.205(h)(2);

(B) Ranging from one to multiple patients; and

(C) That includes all of the data captured for each and every CQM to which technology was certified under paragraph (c)(1)(i) of this section.

(2) *Clinical quality measures—import and calculate*—(i) *Import.* Enable a user to import a data file in accordance with the standard specified in §170.205(h)(2) for one or multiple patients and use such data to perform the capability specified in paragraph (c)(2)(ii) of this section. A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(ii) Calculate each and every clinical quality measure for which it is presented for certification.

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

(i) In accordance with the applicable implementation specifications specified by the CMS implementation guides for Quality Reporting Document Architecture (QRDA), category I, for inpatient measures in §170.205(h)(3) and CMS implementation guide for QRDA, category III for ambulatory measures in §170.205 (k)(3); or

(ii) In accordance with the standards specified in §170.205(h)(2) and §170.205(k)(1) and (2) for the period before December 31, 2022.

(4) *Clinical quality measures—filter.* (i) Record the data listed in paragraph (c)(4)(iii) of this section in accordance with the identified standards, where specified.

(ii) Filter CQM results at the patient and aggregate levels by each one and any combination of the data listed in paragraph (c)(4)(iii) of this section and be able to:

(A) Create a data file of the filtered data in accordance with the standards adopted in §170.205(h)(2) and §170.205(k)(1) and (2); and

(B) Display the filtered data results in human readable format.

(iii) *Data.*

(A) Taxpayer Identification Number.

(B) National Provider Identifier.

(C) Provider type in accordance with, at a minimum, the standard specified in §170.207(r)(1).

(D) Practice site address.

(E) Patient insurance in accordance with the standard specified in §170.207(s)(1).

(F) Patient age.

(G) Patient sex in accordance with the version of the standard specified in §170.207(n)(1).

(H) Patient race and ethnicity in accordance with, at a minimum, the version of the standard specified in §170.207(f)(2).

(I) Patient problem list data in accordance with, at a minimum, the version of the standard specified in §170.207(a)(4).

(d) *Privacy and security*—(1) *Authentication, access control, and authorization.* (i) Verify against a unique identifier(s) (*e.g.*, username or number) that a user 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 technology.

(2) *Auditable events and tamper-resistance*—(i) *Record actions.* 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 technology in accordance with the standard specified in §170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices (see paragraph (d)(7) of this section).

(ii) *Default setting.* 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) and (d)(2)(i)(C) of this section.

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

(v) *Detection.* 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 in §170.210(e).

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

(i) *Accepted amendment.* For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment's location.

(ii) *Denied amendment.* For a denied amendment, at a minimum, append the request and denial of the request in at least one of the following ways:

(A) To the affected record.

(B) Include a link that indicates this information's location.

(5) *Automatic access time-out.* (i) Automatically stop user access to health information after a predetermined period of inactivity.

(ii) Require user authentication in order to resume or regain the access that was stopped.

(6) *Emergency access.* Permit an identified set of users to access electronic health information during an emergency.

(7) *End-user device encryption.* The requirements specified in one of the following paragraphs (that is, paragraphs (d)(7)(i) and (d)(7)(ii) of this section) must be met to satisfy this certification criterion.

(i) Technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of the technology on those devices stops.

(A) Electronic health information that is stored must be encrypted in accordance with the standard specified in §170.210(a)(2).

(B) *Default setting.* Technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users.

(ii) Technology is designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops.

(8) *Integrity.* (i) Create a message digest in accordance with the standard specified in §170.210(c)(2).

(ii) Verify in accordance with the standard specified in §170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.

(9) *Trusted connection.* Establish a trusted connection using one of the following methods:

(i) *Message-level.* Encrypt and integrity protect message contents in accordance with the standards specified in §170.210(a)(2) and (c)(2).

(ii) *Transport-level.* Use a trusted connection in accordance with the standards specified in §170.210(a)(2) and (c)(2).

(10) *Auditing actions on health information.* (i) By default, be set to record actions related to electronic health information in accordance with the standard specified in §170.210(e)(1).

(ii) If technology permits auditing to be disabled, the ability to do so must be restricted to a limited set of users.

(iii) Actions recorded related to electronic health information must not be

capable of being changed, overwritten, or deleted by the technology.

(iv) Technology must be able to detect whether the audit log has been altered.

(11) *Accounting of disclosures.* Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(d).

(12) *Encrypt authentication credentials.* Health IT developers must make one of the following attestations and may provide the specified accompanying information, where applicable:

(i) Yes—the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).

(ii) No—the Health IT Module does not encrypt stored authentication credentials. When attesting ''no,'' the health IT developer may explain why the Health IT Module does not support encrypting stored authentication credentials.

(13) *Multi-factor authentication.* Health IT developers must make one of the following attestations and, as applicable, provide the specified accompanying information:

(i) Yes—the Health IT Module supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting ''yes,'' the health IT developer must describe the use cases supported.

(ii) No—the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting ''no,'' the health IT developer may explain why the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards.

(e) *Patient engagement*—(1) *View, download, and transmit to 3rd party.* (i) Patients (and their authorized representatives) must be able to use internet-based technology to view, download, and transmit their health information to a 3rd party in the manner specified below. Such access must be consistent and in accordance with the standard adopted in § 170.204(a)(1) and may alternatively be demonstrated in accordance with the standard specified in § 170.204(a)(2).

(A) *View.* Patients (and their authorized representatives) must be able to use health IT to view, at a minimum, the following data:

(*1*) The data classes expressed in the standards in § 170.213 (which should be in their English (*i.e.*, non-coded) representation if they associate with a vocabulary/code set), and in accordance with § 170.205(a)(4) and (a)(5), and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iii*) of this section, or

(*2*) The Common Clinical Data Set in accordance with § 170.205(a)(4) and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iv*) of this section for the period before December 31, 2022.

(*3*) The following data classes:

(*i*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4).

(*ii*) *Goals.* In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4).

(*iii*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4).

(*iv*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standards specified in § 170.205(a)(4).

(*4*) Ambulatory setting only. Provider's name and office contact information.

(*5*) Inpatient setting only. Admission and discharge dates and locations; discharge instructions; and reason(s) for hospitalization.

(*6*) Laboratory test report(s). Laboratory test report(s), including:

(*i*) The information for a test report as specified all the data specified in 42 CFR 493.1291(c)(1) through (7);

(*ii*) The information related to reference intervals or normal values as specified in 42 CFR 493.1291(d); and

(*iii*) The information for corrected reports as specified in 42 CFR 493.1291(k)(2).

(*7*) Diagnostic image report(s).

(B) *Download*. (*1*) Patients (and their authorized representatives) must be able to use technology to download an ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) in the following formats:

(*i*) Human readable format; and

(*ii*) The format specified in accordance to the standard specified in §170.205(a)(4) and (5) following the CCD document template.

(*2*) When downloaded according to the standard specified in §170.205(a)(4) and (5) following the CCD document template, the ambulatory summary or inpatient summary must include, at a minimum, the following data (which, for the human readable version, should be in their English representation if they associate with a vocabulary/code set):

(*i*) *Ambulatory setting only*. All of the data specified in paragraph (e)(1)(i)(A)(*1*), (*2*), (*4*), and (*5*) of this section.

(*ii*) *Inpatient setting only*. All of the data specified in paragraphs (e)(1)(i)(A)(*1*), and (*3*) through (*5*) of this section.

(*3*) *Inpatient setting only*. Patients (and their authorized representatives) must be able to download transition of care/referral summaries that were created as a result of a transition of care (pursuant to the capability expressed in the certification criterion specified in paragraph (b)(1) of this section).

(C) *Transmit to third party*. Patients (and their authorized representatives) must be able to:

(*1*) Transmit the ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) created in paragraph (e)(1)(i)(B)(*2*) of this section in accordance with both of the following ways:

(*i*) Email transmission to any email address; and

(*ii*) An encrypted method of electronic transmission.

(*2*) *Inpatient setting only*. Transmit transition of care/referral summaries (as a result of a transition of care/referral as referenced by (e)(1)(i)(B)(*3*)) of this section selected by the patient (or their authorized representative) in both of the ways referenced (e)(1)(i)(C)(*1*)(*i*) and (*ii*) of this section).

(D) *Timeframe selection*. With respect to the data available to view, download, and transmit as referenced paragraphs (e)(1)(i)(A), (B), and (C) of this section, patients (and their authorized representatives) must be able to:

(*1*) Select data associated with a specific date (to be viewed, downloaded, or transmitted); and

(*2*) Select data within an identified date range (to be viewed, downloaded, or transmitted).

(ii) *Activity history log*. (A) When any of the capabilities included in paragraphs (e)(1)(i)(A) through (C) of this section are used, the following information must be recorded and made accessible to the patient (or his/her authorized representative):

(*1*) The action(s) (*i.e.*, view, download, transmission) that occurred;

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

(*3*) The user who took the action; and

(*4*) Where applicable, the addressee to whom an ambulatory summary or inpatient summary was transmitted.

(B) [Reserved]

(2) *Secure messaging*. Enable a user to send messages to, and receive messages from, a patient in a secure manner.

(3) *Patient health information capture*. Enable a user to:

(i) Identify, record, and access information directly and electronically shared by a patient (or authorized representative).

(ii) Reference and link to patient health information documents.

(f) *Public health*—(1) *Transmission to immunization registries*. (i) Create immunization information for electronic transmission in accordance with:

(A) The standard and applicable implementation specifications specified in §170.205(e)(4).

(B) At a minimum, the version of the standard specified in §170.207(e)(3) for historical vaccines.

(C) At a minimum, the version of the standard specified in §170.207(e)(4) for administered vaccines.

(ii) Enable a user to request, access, and display a patient's evaluated immunization history and the immunization forecast from an immunization registry in accordance with the standard at § 170.205(e)(4).

(2) *Transmission to public health agencies—syndromic surveillance.* Create syndrome-based public health surveillance information for electronic transmission in accordance with the standard (and applicable implementation specifications) specified in § 170.205(d)(4).

(3) *Transmission to public health agencies—reportable laboratory tests and values/results.* Create reportable laboratory tests and values/results for electronic transmission in accordance with:

(i) The standard (and applicable implementation specifications) specified in § 170.205(g).

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(3) and (c)(2).

(4) *Transmission to cancer registries.* Create cancer case information for electronic transmission in accordance with:

(i) The standard (and applicable implementation specifications) specified in § 170.205(i)(2).

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(4) and (c)(3).

(5) *Transmission to public health agencies—electronic case reporting.* (i) Consume and maintain a table of trigger codes to determine which encounters may be reportable.

(ii) Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.

(iii) *Case report creation.* Create a case report for electronic transmission:

(A) Based on a matched trigger from paragraph (f)(5)(ii).

(B) That includes, at a minimum:

(*1*) The data classes expressed in the standard in § 170.213, or

(*2*) The Common Clinical Data Set for the period before December 31, 2022.

(*3*) *Encounter diagnoses.* Formatted according to at least one of the following standards:

(*i*) The standard specified in § 170.207(i).

(*ii*) At a minimum, the version of the standard specified in § 170.207(a)(4).

(*4*) The provider's name, office contact information, and reason for visit.

(*5*) An identifier representing the row and version of the trigger table that triggered the case report.

(6) *Transmission to public health agencies—antimicrobial use and resistance reporting.* Create antimicrobial use and resistance reporting information for electronic transmission in accordance with the standard specified in § 170.205(r)(1).

(7) *Transmission to public health agencies—health care surveys.* Create health care survey information for electronic transmission in accordance with the standard specified in § 170.205(s)(1).

(g) *Design and performance*—(1) *Automated numerator recording.* For each Promoting Interoperability Programs percentage-based measure, technology must be able to create a report or file that enables a user to review the patients or actions that would make the patient or action eligible to be included in the measure's numerator. The information in the report or file created must be of sufficient detail such that it enables a user to match those patients or actions to meet the measure's denominator limitations when necessary to generate an accurate percentage.

(2) *Automated measure calculation.* For each Promoting Interoperability Programs percentage-based measure that is supported by a capability included in a technology, record the numerator and denominator and create a report including the numerator, denominator, and resulting percentage associated with each applicable measure.

(3) *Safety-enhanced design.* (i) User-centered design processes must be applied to each capability technology includes that is specified in the following certification criteria: Paragraphs (a)(1) through (5), (9), and (14), and (b)(2) and (3).

(ii) *Number of test participants.* A minimum of 10 test participants must be used for the testing of each capability identified in paragraph (g)(3)(i) of this section.

(iii) One of the following must be submitted on the user-centered design processed used:

(A) Name, description and citation (URL and/or publication citation) for an industry or federal government standard.

(B) Name the process(es), provide an outline of the process(es), a short description of the process(es), and an explanation of the reason(s) why use of any of the existing user-centered design standards was impractical.

(iv) The following information/sections from NISTIR 7742 must be submitted for each capability to which user-centered design processes were applied:

(A) Name and product version; date and location of the test; test environment; description of the intended users; and total number of participants;

(B) Description of participants, including: Sex; age; education; occupation/role; professional experience; computer experience; and product experience;

(C) Description of the user tasks that were tested and association of each task to corresponding certification criteria;

(D) The specific metrics captured during the testing of each user task performed in (g)(3)(iv)(C) of this section, which must include: Task success (%); task failures (%); task standard deviations (%); task performance time; and user satisfaction rating (based on a scale with 1 as very difficult and 5 as very easy) or an alternative acceptable user satisfaction measure;

(E) Test results for each task using the metrics identified above in paragraph (g)(3)(iv)(D) of this section; and

(F) Results and data analysis narrative, including: Major test finding; effectiveness; efficiency; satisfaction; and areas for improvement.

(v) Submit test scenarios used in summative usability testing.

(4) *Quality management system.* (i) For each capability that a technology includes and for which that capability's certification is sought, the use of a Quality Management System (QMS) in the development, testing, implementation, and maintenance of that capability must be identified that satisfies one of the following ways:

(A) The QMS used is established by the Federal government or a standards developing organization.

(B) The QMS used is mapped to one or more QMS established by the Federal government or standards developing organization(s).

(ii) When a single QMS was used for applicable capabilities, it would only need to be identified once.

(iii) When different QMS were applied to specific capabilities, each QMS applied would need to be identified.

(5) *Accessibility-centered design.* For each capability that a Health IT Module includes and for which that capability's certification is sought, the use of a health IT accessibility-centered design standard or law in the development, testing, implementation and maintenance of that capability must be identified.

(i) When a single accessibility-centered design standard or law was used for applicable capabilities, it would only need to be identified once.

(ii) When different accessibility-centered design standards and laws were applied to specific capabilities, each accessibility-centered design standard or law applied would need to be identified. This would include the application of an accessibility-centered design standard or law to some capabilities and none to others.

(iii) When no accessibility-centered design standard or law was applied to all applicable capabilities such a response is acceptable to satisfy this certification criterion.

(6) *Consolidated CDA creation performance.* The following technical and performance outcomes must be demonstrated related to Consolidated CDA creation. The capabilities required under paragraphs (g)(6)(i) through (v) of this section can be demonstrated in tandem and do not need to be individually addressed in isolation or sequentially.

(i) This certification criterion's scope includes:

(A) The data classes expressed in the standard in §170.213, and in accordance with §170.205(a)(4) and (5) and paragraphs (g)(6)(i)(C)(*1*) through (*3*) of this section; or

(B) The Common Clinical Data Set in accordance with §170.205(a)(4) and paragraphs (g)(6)(i)(C)(*1*) through (*4*) of this section for the period before December 31, 2022.

(C) The following data classes:

(*1*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in §170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in §170.205(a)(4).

(*2*) *Goals.* In accordance with the ''Goals Section'' of the standard specified in §170.205(a)(4).

(*3*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standard specified in §170.205(a)(4).

(*4*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in §170.205(a)(4).

(ii) *Reference C–CDA match.* (A) For health IT certified to (g)(6)(i)(A) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) and (5) that matches a gold-standard, reference data file.

(B) For health IT certified to (g)(6)(i)(B) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) that matches a gold-standard, reference data file.

(iii) *Document-template conformance.* (A) For health IT certified to (g)(6)(i)(A) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) and (5) that demonstrates a valid implementation of each document template applicable to the certification criterion or criteria within the scope of the certificate sought.

(B) For health IT certified to (g)(6)(i)(B) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) that demonstrates a valid implementation of each document template applicable to the certification criterion or criteria within the scope of the certificate sought.

(iv) *Vocabulary conformance.* (A) For health IT certified to (g)(6)(i)(A) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) and (5) that demonstrates the required vocabulary standards (and value sets) are properly implemented.

(B) For health IT certified to (g)(6)(i)(B) of this section, create a data file formatted in accordance with the standard adopted in §170.205(a)(4) that demonstrates the required vocabulary standards (and value sets) are properly implemented.

(v) *Completeness verification.* Create a data file for each of the applicable document templates referenced in paragraph (g)(6)(iii) of this section without the omission of any of the data included in either paragraph (g)(6)(i)(A) or (B) of this section, as applicable.

(7) *Application access—patient selection.* The following technical outcome and conditions must be met through the demonstration of an application programming interface (API).

(i) *Functional requirement.* The technology must be able to receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient's data.

(ii) *Documentation.* (A) The API must include accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(B) The documentation used to meet paragraph (g)(7)(ii)(A) of this section must be available via a publicly accessible hyperlink.

(8) *Application access—data category request.* The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) *Functional requirements.* (A) Respond to requests for patient data (based on an ID or other token) for each of the individual data categories

specified in the Common Clinical Data Set and return the full set of data for that data category (according to the specified standards, where applicable) in a computable format.

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(ii) *Documentation*—(A) The API must include accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(B) The documentation used to meet paragraph (g)(8)(ii)(A) of this section must be available via a publicly accessible hyperlink.

(9) *Application access—all data request.* The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) *Functional requirements.* (A)(*1*) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in §170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with §170.205(a)(4) and (5) following the CCD document template, and as specified in paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iii*) of this section, or

(*2*) The Common Clinical Data Set in accordance with paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iv*) of this section for the period before December 31, 2022, and

(*3*) The following data classes:

(*i*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standards specified in §170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standards specified in §170.205(a)(4).

(*ii*) *Goals.* In accordance with the ''Goals Section'' of the standards specified in §170.205(a)(4).

(*iii*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standards specified in §170.205(a)(4).

(*iv*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standards specified in §170.205(a)(4).

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(ii) *Documentation*—(A) The API must include accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(B) The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

(10) *Standardized API for patient and population services.* The following technical outcomes and conditions must be met through the demonstration of application programming interface technology.

(i) *Data response.* (A) Respond to requests for a single patient's data according to the standard adopted in §170.215(a)(1) and implementation specification adopted in §170.215(a)(2), including the mandatory capabilities described in ''US Core Server CapabilityStatement,'' for each of the data included in the standard adopted in §170.213. All data elements indicated as ''mandatory'' and ''must support'' by the standards and implementation specifications must be supported.

(B) Respond to requests for multiple patients' data as a group according to the standard adopted in §170.215(a)(1), and implementation specifications adopted in §170.215(a)(2) and (4), for

each of the data included in the standard adopted in §170.213. All data elements indicated as ''mandatory'' and ''must support'' by the standards and implementation specifications must be supported.

(ii) *Supported search operations.* (A) Respond to search requests for a single patient's data consistent with the search criteria included in the implementation specification adopted in §170.215(a)(2), specifically the mandatory capabilities described in ''US Core Server CapabilityStatement.''

(B) Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in §170.215(a)(4).

(iii) *Application registration.* Enable an application to register with the Health IT Module's ''authorization server.''

(iv) *Secure connection.* (A) Establish a secure and trusted connection with an application that requests data for patient and user scopes in accordance with the implementation specifications adopted in §170.215(a)(2) and (3).

(B) Establish a secure and trusted connection with an application that requests data for system scopes in accordance with the implementation specification adopted in §170.215(a)(4).

(v) *Authentication and authorization*—(A) *Authentication and authorization for patient and user scopes*—(*1*) *First time connections.* (*i*) Authentication and authorization must occur during the process of granting access to patient data in accordance with the implementation specification adopted in §170.215(a)(3) and standard adopted in §170.215(b).

(*ii*) A Health IT Module's authorization server must issue a refresh token valid for a period of no less than three months to applications capable of storing a client secret.

(*iii*) A Health IT Module's authorization server must issue a refresh token for a period of no less than three months to native applications capable of securing a refresh token

(*2*) *Subsequent connections.* (*i*) Access must be granted to patient data in accordance with the implementation specification adopted in §170.215(a)(3) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application.

(*ii*) A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications capable of storing a client secret.

(B) *Authentication and authorization for system scopes.* Authentication and authorization must occur during the process of granting an application access to patient data in accordance with the ''SMART Backend Services: Authorization Guide'' section of the implementation specification adopted in §170.215(a)(4) and the application must be issued a valid access token.

(vi) *Patient authorization revocation.* A Health IT Module's authorization server must be able to revoke an authorized application's access at a patient's direction.

(vii) *Token introspection.* A Health IT Module's authorization server must be able to receive and validate tokens it has issued.

(viii) *Documentation.* (A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(*3*) All applicable technical requirements and attributes necessary for an application to be registered with a Health IT Module's authorization server.

(B) The documentation used to meet paragraph (g)(10)(viii)(A) of this section must be available via a publicly accessible hyperlink without any preconditions or additional steps.

(h) *Transport methods and other protocols*—(1) *Direct Project*—(i) *Applicability Statement for Secure Health Transport.* Able to send and receive health information in accordance with the standard specified in §170.202(a)(2), including formatted only as a ''wrapped'' message.

(ii) *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in §170.202(e)(1).

(2) *Direct Project, Edge Protocol, and XDR/XDM.* (i) Able to send and receive health information in accordance with:

(A) The standard specified in §170.202(a)(2), including formatted only as a ''wrapped'' message;

(B) The standard specified in §170.202(b), including support for both limited and full XDS metadata profiles; and

(C) Both edge protocol methods specified by the standard in §170.202(d).

(ii) *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in §170.202(e)(1).

[80 FR 62747, Oct. 16, 2015, as amended at 80 FR 76871, Dec. 11, 2015; 85 FR 25941, May 1, 2020; 85 FR 47099, Aug. 4, 2020; 85 FR 70083, Nov. 4, 2020; 85 FR 78236, Dec. 4, 2020]

Subpart D—Conditions and Maintenance of Certification Requirements for Health IT Developers

SOURCE: 85 FR 25945, May 1, 2020, unless otherwise noted.

§170.400 Basis and scope.

This subpart implements section 3001(c)(5)(D) of the Public Health Service Act by setting forth certain Conditions and Maintenance of Certification requirements for health IT developers participating in the ONC Health IT Certification Program.

§170.401 Information blocking.

(a) *Condition of Certification requirement.* A health IT developer must not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and §171.103 on or after April 5, 2021.

(b) [Reserved]

[85 FR 25945, May 1, 2020, as amended at 85 FR 70084, Nov. 4, 2020]

§170.402 Assurances.

(a) *Condition of Certification requirement.* (1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and §171.103 of this chapter on and after April 5, 2021, unless for legitimate purposes as specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information.

(2) A health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria.

(3) A health IT developer must not take any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the full scope of the technology's certification.

(4) A health IT developer of a certified Health IT Module that is part of a health IT product which electronically stores EHI must certify to the certification criterion in §170.315(b)(10).

(b) *Maintenance of Certification requirements.* (1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for:

(i) A period of 10 years beginning from the date a developer's Health IT Module(s) is first certified under the Program; or

(ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.

(2)(i) By December 31, 2023, a health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in §170.315(b)(10).

(ii) On and after December 31, 2023, a health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in §170.315(b)(10).

[85 FR 25945, May 1, 2020, as amended at 85 FR 70084, Nov. 4, 2020; 85 FR 70084, Nov. 4, 2020]