ONC Stage 2 to EHNAC Comparison:
Summary of Matches

45 CFR Subtitle A, Subchapter D, Part 170 Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology		Key: YELLOW indicates minor correlation: The EHNAC Criteria noted in this program has some similarity to the ONC EHR Stage 2 criteria. RED indicates Major correlation: The EHNAC Criteria noted in this program coincide with the ONC EHR Stage 2 criteria.
ONC Certification Criteria Stage 2 Reference	ONC Certification Criteria Stage 2	EHNAC Relevance
§170.314 (a)(1) Computerized provider order en	Enable a user to electronically record, change, and access the following order types, at a minimum: (i) Medications; (ii) Laboratory; and (iii) Radiology/imaging.	Section VII.A. Pharmacy Application requirements. Several criteria.
§170.314 (a)(3)(i) Demographics.	Enable a user to electronically record, change, and access patient demographic data including preferred language, sex, race, ethnicity, and date of birth. (A) Enable race and ethnicity to be recorded in accordance with the OMB Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15 as revised, October 30, 1997 and whether a patient declines to specify race and/or ethnicity. (B) Enable preferred language to be recorded in accordance with the standard specified in § 170.207(g) and whether a patient declines to specify a preferred language.	Section VII.D criteria
§170.314 (a)(3)(ii) Demographics.	Inpatient setting only. Enable a user to electronically record, change, and access preliminary cause of death in the event of a mortality.	Section VII.D criteria
§170.314 (a)(6) Medication List.	Enable a user to electronically record, change, and access a patient's active medication list as well as medication history:	VII. A.7 [MANDATORY] The electronic prescription application must be capable of recording all of the applicable information required in part 1306 of 21 CFR chapter II for the controlled substance prescription. {632} 21 C.F.R. § 1311.120(b)(6)
§170.314 (a)(6)(i) Medication List.	Ambulatory setting. Over multiple encounters	VII. A.7 [MANDATORY] The electronic prescription application must be capable of recording all of the applicable information required in part 1306 of 21 CFR chapter II for the controlled substance prescription. {632} 21 C.F.R. § 1311.120(b)(6)
§170.314 (a)(6)(ii) Medication List.	Inpatient setting. For the duration of an entire hospitalization.	VII. A.7 [MANDATORY] The electronic prescription application must be capable of recording all of the applicable information required in part 1306 of 21 CFR chapter II for the controlled substance prescription. {632} 21 C.F.R. § 1311.120(b)(6)
§170.314 (a)(7) Medication Allergy List.	Enable a user to electronically record, change, and access a patient's active medication allergy list as well as medication allergy history	VII. A.7 [MANDATORY] The electronic prescription application must be capable of recording all of the applicable information required in part 1306 of 21 CFR chapter II for the controlled substance prescription. {632} 21 C.F.R. § 1311.120(b)(6)
§170.314 (a)(7)(i) Medication Allergy List.	Ambulatory setting. Over multiple encounters	VII. A.7 [MANDATORY] The electronic prescription application must be capable of recording all of the applicable information required in part 1306 of 21 CFR chapter II for the controlled substance prescription. {632} 21 C.F.R. § 1311.120(b)(6)
§170.314 (a)(7)(ii) Medication Allergy List.	Inpatient setting. For the duration of an entire hospitalization.	VII. A.7 [MANDATORY] The electronic prescription application must be capable of recording all of the applicable information required in part 1306 of 21 CFR chapter II for the controlled substance prescription. {632} 21 C.F.R. § 1311.120(b)(6)
§170.314 (a)(15) Patient-specific Education Resources.	EHR technology must be able to electronically identify for a user patient-specific education resources based on data included in the patient's problem list, medication list, and laboratory tests and values/results:	XII.A.3 - Candidate must provide to patients clinical educational materials and ACO educational materials. {1318}
§170.314 (b)(1)(i) Care coordination. Transitions of care—receive, display, and incorporate transition of care/referral summaries. Receive.	Receive. EHR technology must be able to electronically receive transition of care/referral summaries in accordance with: (A) The standard ONC Applicability Statement for Secure Health Transport. (B) Optional. The standards ONC Applicability Statement for Secure Health Transport and ONC XDR and XDM for Direct Messaging Specification. (C) Optional. The standards ONC XDR and XDM for Direct Messaging Specification and ONC Transport and Security Specification.	VI. A.1 [MANDATORY] Candidate's HISP Services must perform authentication, encryption, and trust verification using SMTP transport protocol as specified in the Applicability Statement for Direct Secure Health Transport in order to securely route messages from sender's address to intended recipient's address. {1282}
§170.314 (b)(1)(ii) Care coordination. Transitions of care—receive, display, and incorporate transition of care/referral summaries. Display.	EHR technology must be able to electronically display in human readable format the data included in transition of care/referral summaries received and formatted according to any of the following standards (and applicable implementation specifications) specified here: Health Level Seven Clinical Document Architecture (CDA) Release 2, Continuity of Care Document (CCD), ASTM E2369 Standard Specification for Continuity of Care Record and Adjunct to ASTM E2369, and HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation.	XV.A - Coordination of Care - Multiple critiera.
§170.314 (b)(1)(iii) Care coordination. Transitions of care—receive, display, and incorporate transition of care/referral summaries. Incorporate.	Upon receipt of a transition of care/referral summary formatted according to the standard HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, EHR technology must be able to:	XV.A - Coordination of Care - Multiple critiera. No standards based criteria in this section of the EHNAC criteria however.
§170.314 (b)(1)(iii)(A) Care coordination. Transitions of care—receive, display, and incorporate transition of care/referral summaries. Incorporate.	Correct patient. Demonstrate that the transition of care/referral summary received is or can be properly matched to the correct patient.	XV.A - Coordination of Care - EHNAC criteria do not drill down into the details as deeply as the ONC criteria.
§170.314 (b)(1)(iii)(B) Care coordination. Transitions of care—receive, display, and incorporate transition of care/referral summaries. Incorporate.	Data incorporation. Electronically incorporate the following data expressed according to the specified standard(s): (1) Medications. At a minimum, the version of the standard RxNorm; (2) Problems. At a minimum, the version of the standard IHTSDO SNOMED CT® International Release July 2012; (3) Medication allergies. At a minimum, the version of the standard RxNorm.	XV.A - Coordination of Care - EHNAC criteria do not drill down into the details as deeply as the ONC criteria.
§170.314 (b)(1)(iii)(C) Care coordination. Transitions of care—receive, display, and incorporate transition of care/referral summaries. Incorporate.	Section views. Extract and allow for individual display each additional section or sections (and the accompanying document header information) that were included in a transition of care/referral summary received and formatted in accordance with the standard HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation.	XV.A - Coordination of Care - EHNAC criteria do not drill down into the details as deeply as the ONC criteria.

ONC Stage 2 to EHNAC Comparison:
Summary of Matches

ONC Certification Criteria Stage 2 Reference	ONC Certification Criteria Stage 2	EHNAC Relevance
§170.314 (b)(2)(ii) Transitions of care—create and transmit transition of care/referral summaries. Transmit.	Transmit. Enable a user to electronically transmit the transition of care/referral summary created in paragraph (b)(2)(i) of this section in accordance with the following standards: (A) The standard ONC Applicability Statement for Secure Health Transport. (B) Optional. The standards ONC Applicability Statement for Secure Health Transport and ONC XDR and XDM for Direct Messaging Specification. (C) Optional. The standards ONC XDR and XDM for Direct Messaging Specification and ONC Transport and Security Specification.	VI. A.1 [MANDATORY] Candidate's HISP Services must perform authentication, encryption, and trust verification using SMTP transport protocol as specified in the Applicability Statement for Direct Secure Health Transport in order to securely route messages from sender's address to intended recipient's address. {1282}
§170.314 (b)(3) Electronic Prescribing.	Enable a user to electronically create prescriptions and prescription-related information for electronic transmission in accordance with: (i) The NCPDP SCRIPT Standard, Implementation Guide, Version 10.6; and (ii) At a minimum, RxNorm August 6, 2012 version.	III. E.1 Candidate must have the capability to handle generally accepted industry standard formats, e.g. NCPDP, X12, HL7, for new prescriptions and renewals and support additional standards as they are adopted by the industry. {379}
§170.314 (b)(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):	IV.A.4 [MANDATORY] (G) Candidate must ensure that customers receive documentation that approximates the time, financial, and other resources necessary to import/export patient data if the customer wishes to migrate to/from the candidate's software. {1458}
§170.314 (b)(7)(i) Data Portability.	Encounter diagnoses. The ICD-9 standard or, at a minimum, the version of the standard IHTSDO SNOMED CT® International Release July 2012.	VIII.B.1 [MANDATORY] (G) Candidate must demonstrate the ability to support a charge entry using CPT, HCPCS, and ICD-9CM/ICD-10CM. {1372}
§170.314 (c)(1)(i) Clinical quality measures. Clinical Quality Measures—capture and export.	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 Clinical quality measure-by-measure data, Data Element Catalog 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.''	XIII.A.1 - Candidate must maintain an ACO Quality Measurement program that measures and communicates the performance of the ACO on a regular basis to participating providers. {1320}
§170.314 (c)(1)(ii) Clinical quality measures. Clinical Quality Measures—capture and export.	Export. EHR technology must be able to electronically export a data file formatted in accordance with CQM HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture 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.	XIII.A.1 - Candidate must maintain an ACO Quality Measurement program that measures and communicates the performance of the ACO on a regular basis to participating providers. {1320}
§170.314 (c)(2)(i) Clinical quality measures. Import and Calculate.	Import. EHR technology must be able to electronically import a data file formatted in accordance with CQM HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture 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).	VII.D and VII.E sections related to PQRS and QCDR registries
§170.314 (c)(2)(ii) Clinical quality measures. Import and Calculate.	Calculate. EHR technology must be able to electronically calculate each and every clinical quality measure for which it is presented for certification.	XIII.A.1 - Candidate must maintain an ACO Quality Measurement program that measures and communicates the performance of the ACO on a regular basis to participating providers. {1320}
§170.314 (c)(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 CQM HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture and Clinical quality measure aggregate electronic submission Quality Reporting Document Architecture Category III Implementation Guide for CDA Release 2; and (ii) That can be electronically accepted by CMS.	XIII.A.1 - Candidate must maintain an ACO Quality Measurement program that measures and communicates the performance of the ACO on a regular basis to participating providers. {1320}
§170.314 (d)(1)(i) Privacy and security. Authentication, access control, and authorization.	Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed;	VI.D.2 - Candidate must assign a unique name and/or number for identifying and tracking all systems' user identity. {566} 45 C.F.R. § 164.312(a)(2)(i)
§170.314 (d)(1)(ii) Privacy and security. Authentication, access control, and authorization.	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.	VI. D.1 [MANDATORY] Candidate must implement technical policies and procedures for electronic information systems that maintain Electronic PHI to allow access only to those persons or software programs that have been granted access rights. {889} 45 C.F.R. § 164.312(a)(1)
§170.314 (d)(2)(i) Privacy and security. Auditable events and tamper resistance.	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).	XI. A.1 Candidate must have policies for the maintenance of disclosure logs by the ACO and/or participating organizations for the systems at which authorized users access PHI, including: - The identity of the patient whose PHI was accessed; - The identity of the authorized user accessing the PHI; - The identity of the trading partner with which such authorized user is affiliated; - The type of PHI or record accessed (e.g., pharmacy data, laboratory data, etc.); - The date and time of access; and - The source of the PHI (i.e., the identity of the trading partner from whose records the accessed PHI was derived). {1275}
§170.314 (d)(2)(ii) Privacy and security. Auditable events and tamper resistance.	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).	XI. A.1 Candidate must have policies for the maintenance of disclosure logs by the ACO and/or participating organizations for the systems at which authorized users access PHI, including: - The identity of the patient whose PHI was accessed; - The identity of the authorized user accessing the PHI; - The identity of the trading partner with which such authorized user is affiliated; - The type of PHI or record accessed (e.g., pharmacy data, laboratory data, etc.); - The date and time of access; and - The source of the PHI (i.e., the identity of the trading partner from whose records the accessed PHI was derived). {1275}

ONC Stage 2 to EHNAC Comparison:
Summary of Matches

ONC Certification Criteria Stage 2 Reference	ONC Certification Criteria Stage 2	EHNAC Relevance
§170.314 (d)(2)(iii) Privacy and security. Auditable events and tamper resistance.	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.	VIII. A.1 [MANDATORY] The application provider must establish and implement a list of auditable events. Auditable events must, at a minimum, include the following: (1) Attempted unauthorized access to the electronic prescription application, or successful unauthorized access where the determination of such is feasible. (2) Attempted unauthorized modification or destruction of any information or records required by § 1311, or successful unauthorized modification or destruction of any information or records required by § 1311 where the determination of such is feasible. (3) Interference with application operations of the prescription application. (4) Any setting of or change to logical access controls related to the issuance of controlled substance prescriptions. (5) Attempted or successful interference with audit trail functions. (6) For application service providers, attempted or successful creation, modification, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider. {668} 21 C.F.R. § 1311.150(a)
§170.314 (d)(2)(iv) Privacy and security. Auditable events and tamper resistance.	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.	XI. A.2 Candidate must have controls that secure disclosure logs from alteration regardless of access privilege and that log any attempted alterations. {1276}
§170.314 (d)(2)(v) Privacy and security. Auditable events and tamper resistance.	Detection. EHR technology must be able to detect whether the audit log has been altered.	V. B.3 Candidate must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports and maintain/report discrepancies to the security officer for review. {610} 45 C.F.R §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C)
§170.314 (d)(3) Audit Reports.	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).	V. B.3 Candidate must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports and maintain/report discrepancies to the security officer for review. {610} 45 C.F.R §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C)
§170.314 (d)(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.	XII. A.1 Candidate must, if it provides or supports personal health records, provide the ability for patients to view and contribute information to their personal health record if one is available to the patient. {1404}
§170.314 (d)(5) Automatic log-off	Prevent a user from gaining further access to an electronic session after a predetermined time of inactivity.	VI. D.4 Candidate must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. {591} 45 C.F.R. § 164.312(a)(2)(iii)
§170.314 (d)(6) Emergency Access	Permit an identified set of users to access electronic health information during an emergency.	VI. D.3 Candidate must establish procedures for accessing necessary Electronic PHI during an emergency. {280} 45 C.F.R. § 164.312(a)(2)(ii)
§170.314 (d)(7)(i) End User Device Encryption	EHR 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 EHR technology on those devices stops.	II. A.8 [MANDATORY] Candidate must have policies in place that prohibit individuals from storing unencrypted PHI on portable devices. {1388} 45 CFR §§ 164.530©
§170.314 (d)(7)(i)(A) End User Device Encryption	Electronic health information that is stored must be encrypted in accordance with the FIPS 140-2 standard.	II. A.8 [MANDATORY] Candidate must have policies in place that prohibit individuals from storing unencrypted PHI on portable devices. {1388} 45 CFR §§ 164.530©
§170.314 (d)(7)(i)(B) End User Device Encryption	Default setting. EHR 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. A.8 [MANDATORY] Candidate must have policies in place that prohibit individuals from storing unencrypted PHI on portable devices. {1388} 45 CFR §§ 164.530©
§170.314 (d)(8)(i) Integrity	Create a message digest in accordance with the SHA-1 hashing standard or greater.	II. A.5 [MANDATORY] Candidate must utilize strong encryption, user authentication, message integrity, and support for non-repudiation as security measures in compliance with any legislation requiring it. {450} HITECH § 13402(h); 45 C.F.R. §§ 164.312(a)(2)(iv), 164.312 (e)(2)(ii)
§170.314 (d)(8)(ii) Integrity	Verify in accordance with the SHA-1 hashing standard or greater, upon receipt of electronically exchanged health information that such information has not been altered.	II. A.5 [MANDATORY] Candidate must utilize strong encryption, user authentication, message integrity, and support for non-repudiation as security measures in compliance with any legislation requiring it. {450} HITECH § 13402(h); 45 C.F.R. §§ 164.312(a)(2)(iv), 164.312 (e)(2)(ii)
§170.314 (d)(9) Optional - Accounting of Disclosures.	Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(d).	VI. E.7 Candidate must require that all Business Associates notify the Candidate in the event any PHI is improperly used or disclosed, including for the purpose of the breach notification rule.{491} HITECH §13404(b), 45 CFR §§ 164.314(a)(2)(i)(C)
§170.314 (e)(1)(i) Patient Engagement. View, download, and transmit to third party.	EHR technology must provide patients (and their authorized representatives) with an online means to view, download, and transmit to a 3rd party the data specified below. Access to these capabilities must be through a secure channel that ensures all content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified in the FIPS 140-2 standard.	XII. A.1 Candidate must, if it provides or supports personal health records, provide the ability for patients to view and contribute information to their personal health record if one is available to the patient. {1404}
§170.314 (e)(1)(i)(A) Patient Engagement. View, download, and transmit to third party.	View. Electronically view in accordance with the Web Content Accessibility Guidelines (WCAG) 2.0 Level A Conformance, at a minimum, the following data: (1) The Common MU Data Set (which should be in their English (i.e., noncoded) representation if they associate with a vocabulary/code set). (2) Ambulatory setting only. Provider's name and office contact information. (3) Inpatient setting only. Admission and discharge dates and locations; discharge instructions; and reason(s) for hospitalization.	XII. A.1 Candidate must, if it provides or supports personal health records, provide the ability for patients to view and contribute information to their personal health record if one is available to the patient. {1404}
§170.314 (e)(1)(i)(B)(1) Patient Engagement. View, download, and transmit to third party.	Download. Electronically download an ambulatory summary or inpatient summary (as applicable to the EHR technology setting for which certification is requested) in human readable format or formatted according to the HL7 2.5.1 IG for CDA Release 2: IHE Health Story Consolidation that includes, 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):	XII. A.1 Candidate must, if it provides or supports personal health records, provide the ability for patients to view and contribute information to their personal health record if one is available to the patient. {1404}
§170.314 (e)(1)(ii)(A)Activity History Log.	When electronic health information is viewed, downloaded, or transmitted to a third-party using the capabilities included in paragraphs (e)(1)(i)(A) through (C) of this section, the following information must be recorded and made accessible to the patient: (1) The action(s) (i.e., view, download, transmission) that occurred; (2) The date and time each action occurred in accordance with the RFC 1305 Network Time Protocol or RFC 5905 Network Time Protocol Version 4 standard; and (3) The user who took the action.	VI. B.3 Candidate must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports and maintain/report discrepancies to the security officer for review. {610} 45 C.F.R §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C)

ONC Stage 2 to EHNAC Comparison:
Summary of Matches

ONC Certification Criteria Stage 2 Reference	ONC Certification Criteria Stage 2	EHNAC Relevance
§170.314 (e)(1)(ii)(B)Activity History Log.	EHR technology presented for certification may demonstrate compliance with paragraph (e)(1)(ii)(A) of this section if it is also certified to the certification criterion adopted at § 170.314(d)(2) and the information required to be recorded in paragraph (e)(1)(ii)(A) is accessible by the patient.	VI. B.3 and XI. A.1 (G) The HIE must have policies for the maintenance of disclosure logs by the HIE and/or participating organizations for the systems at which authorized users access PHI, including: - The identity of the patient whose PHI was accessed; - The identity of the authorized user accessing the PHI; - The identity of the trading partner with which such authorized user is affiliated; - The type of PHI or record accessed (e.g., pharmacy data, laboratory data, etc.); - The date and time of access; and - The source of the PHI (i.e., the identity of the trading partner from whose records the accessed PHI was derived). {588}
§170.314 (e)(3) Ambulatory setting only—secure messaging.	Enable a user to electronically send messages to, and receive messages from, a patient in a manner that ensures: (i) Both the patient (or authorized representative) and EHR technology user are authenticated; and (ii) The message content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms compliant with FIPS 140-2.	II. A.5 [MANDATORY] (G) Candidate must utilize strong encryption, user authentication, message integrity, and support for non-repudiation as security measures in compliance with any legislation requiring it. {450} HITECH § 13402(h); 45 C.F.R. §§ 164.312(a)(2)(iv), 164.312 (e)(2)(ii)
§170.314 (f)(1) Public health. Immunization information.	Enable a user to electronically record, change, and access immunization information.	VII.D and VII.E sections related to PQRS and QCDR registries
§170.314 (f)(2) Public health. Immunization information.	Transmission to immunization registries. EHR technology must be able to electronically create immunization information for electronic transmission in accordance with: (i) The standard and applicable implementation specifications for HL7 2.5.1 IG for Immunization Messaging Release 1.4; and (ii) At a minimum, the version of the HL7 Standard Code Set CVX - Vaccines Administered, updates through July 11, 2012.	VII.D and VII.E sections related to PQRS and QCDR registries
§170.314 (f)(3) Transmission to public health agencies - syndromic surveillance.	EHR technology must be able to electronically create syndrome-based public health surveillance information for electronic transmission in accordance with: (i) Ambulatory setting only. (A) The HL7 2.5.1 standard. (B) Optional. The HL7 2.5.1 IG for Immunization Messaging, Release 1.4 standard. (ii) Inpatient setting only. The HL7 2.5.1 IG for Immunization Messaging, Release 1.4 standard.	Section XIV - Population Health Management and Reporting.
§170.314 (f)(4) Inpatient setting only—transmission of reportable laboratory tests and values/results.	EHR technology must be able to electronically create reportable laboratory tests and values/results for electronic transmission in accordance with: (i) HL7 2.5.1 IG Electronic Laboratory Reporting to Public Health, Release 1; and (ii) At a minimum, the versions of the standards IHTHDSO SNOMED CT March 2012 release and LOINC Database version 2.40.	Section XIV - Population Health Management and Reporting.
§170.314 (f)(5) Optional - Ambulatory Setting only - Cancer Case Information.	Enable a user to electronically record, change, and access cancer case information.	VII.D and VII.E sections related to PQRS and QCDR registries
§170.314 (f)(6) Optional - Ambulatory Setting only - Transmission to Cancer Registries.	EHR technology must be able to electronically create cancer case information for electronic transmission in accordance with: (i) The HL7 CDA Release 2.0 Normative Edition and IG for Ambulatory Healthcare Provider Reporting to Central Cancer Registries, HL7 CDA; and (ii) At a minimum, the versions of the standards IHTHDSO SNOMED CT March 2012 release and LOINC Database version 2.40.	Section XIV - Population Health Management and Reporting.