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

i. 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 at § 170.210(f).

Work Description	The patient portal is already HTTP Secure. The application should check for whether the request comes from browsers that support minimum AES 256, if else have to close the connection.
Standards	**§ 170.210(f)** Encryption and hashing of electronic health information. Any encryption and hashing algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the FIPS Publication 140-2 (incorporated by reference in § 170.299).
Reference Links	http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf
Status	Pending

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

Work Description	Status of MU2 dataset in the patient portal is marked in the tables available in the bottom of this document. Works for Level A conformance of WCAG 2.0 are remaining
Standards	**§ 170.204 (a)** Accessibility. Standard. Web Content Accessibility Guidelines (WCAG) 2.0, Level A Conformance (incorporated by reference in § 170.299).
Reference Links	http://www-static.shell.com/content/dam/shell/static/usa/downloads/footer/wcag-guidelines-1208.pdf http://www.w3.org/WAI/WCAG20/glance/WCAG2-at-a-Glance.pdf
Status	Partially Completed

1. The Common MU Data Set (which should be in their English (i.e., non-coded) representation if they associate with a vocabulary/code set).

Work Description	Care plan field(s), including goals and instructions is missing. (Refer Table 1: Common MU Data Set at the bottom of this document)
Referenced Standards	
Reference Links	http://wiki.siframework.org/file/view/MU2 Data Requirements.docx/360279112/MU2 Data Requirements.docx
Status	Partially Completed

2. Ambulatory setting only. Provider's name and office contact information.

Work Description	For remaining fields to be included in patient portal Refer Table2: Ambulatory or Inpatient Summary at the bottom of this document
Referenced Standards	
Reference Links	
Status	Partially Completed

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

NOT APPLICABLE

B. Download

1. 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 standard adopted at § 170.205(a)(3) 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):

Work Description	Patient portal should have the option for downloading health information (that was viewed as part of the "View") in human readable format and in C-CDA format. Also one should be able to download ambulatory summary and transition care summary separately or together Also the application should check for whether the download request comes from browsers that support minimum AES 256
Referenced Standards	**§ 170.205(a)(3)** :. HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, (incorporated by reference in § 170.299). The use of the "unstructured document" document-level template is prohibited.
Reference Links	http://www.healthit.gov/sites/default/files/glidepath_hitsp_c83_to_ccda.pdf
Status	Pending

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

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

NOT APPLICABLE

2. Inpatient setting only. Electronically 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 adopted at paragraph (b)(2) of this section).

NOT APPLICABLE

C. Transmit to third party.

1. Electronically transmit the ambulatory summary or inpatient summary (as applicable to the EHR technology setting for which certification is requested) created in paragraph (e)(1)(i)(B)(1) of this section in accordance with the standard specified in § 170.202(a)

Work Description	Patient portal should have the option to transmit the health information through a secure channel (Patient portal have to be integrated with emrdirect)
Referenced Standards	**170.202(a).** : ONC Applicability Statement for Secure Health Transport (incorporated by reference in § 170.299).
Reference Links	http://www.himssehra.org/docs/ EHRAStage2SecureHealthTransportCertificationandMeaningfulUse.pdf
Status	Pending

.

2. Inpatient setting only. Electronically transmit transition of care/referral summaries (as a result of a transition of care/referral) selected by the patient (or their authorized representative) in accordance with the standard specified in § 170.202(a).

NOT APPLICABLE

ii. Activity history log.

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

Work Description	Open EMR should keep log of every single action (with health information of a patient) (view/download and transmit) along with the date and time and the user's (who does the action) information. The same log should be made available through the patient portal.

Referenced Standards	**170.210(g):** Synchronized clocks. The date and time recorded utilize a system clock that has been synchronized following (RFC 1305) Network Time Protocol, (incorporated by reference in § 170.299) or (RFC 5905) Network Time Protocol Version 4, (incorporated by reference in § 170.299). (g) Synchronized clocks. The date and time recorded utilize a system clock that has been synchronized following (RFC 1305) Network Time Protocol, (incorporated by reference in § 170.299) or (RFC 5905) Network Time Protocol Version 4, (incorporated by reference in § 170.299).
Reference Links	http://www.rfc-base.org/txt/rfc-1305.txt
Status	Pending

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 at §170.210(g); and
3. The user who took the action.

B. 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.

Work Description	170.314(d)(2)(i)(A) : The **OpenEMR** should record actions on patient data with the following data Date and Time of Event, Patient Identification, User Identification, Access Device (optional), Type of Action (additions, deletions, changes, queries, print, copy), Identification of the Patient Data that is Accessed(optional). And also this data should be made available to patient portal 170.314(d)(2)(i)(B): In OpenEMR an additional type of log should be kept in audit log table to keep track while each time audit log is enabled or disabled While completing 170.314(d)**(2)(i)**, the requirement in 170.314(d)**(2)(ii)** will be met, but should make verify the same **OpenEMR** is already conformance to 170.314(d)**(2)(iii)**, 170.314(d)**(2)(iv)** and 170.314(d)**(2)(v)**

Referenced Standards	**170.314(d)(2)** Auditable events and tamper-resistance. (i) Record actions. EHR technology must be able to: (A) Record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1); (B) Record the audit log status (enabled or disabled) in accordance with the standard specified in § 170.210(e)(2) unless it cannot be disabled by any user; and (C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by EHR technology in accordance with the standard specified in § 170.210(e)(3) unless the EHR technology prevents electronic health information from being locally stored on end-user devices (see 170.314(d)(7) of this section). (ii) Default setting. EHR technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) or (d)(2)(i)(C), or both paragraphs (d)(2)(i)(B) and (C). (iii) When disabling the audit log is permitted. For each capability specified in paragraphs (d)(2)(i)(A), (B), and (C) of this section that EHR technology permits to be disabled, the ability to do so must be restricted to a limited set of identified users. (iv) Audit log protection. Actions and statuses recorded in accordance with paragraph (d)(2)(i) must not be capable of being changed, overwritten, or deleted by the EHR technology. (v) Detection. EHR technology must be able to detect whether the audit log has been altered. **§ 170.210 Standards for health information technology** to protect electronic health information created, maintained, and exchanged. The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged: (e)(1) Record actions related to electronic health information, audit log status, and encryption of end-user devices. (i) The audit log must record the information specified in sections 7.2 through 7.4, 7.6, and 7.7 of the standard specified at § 170.210(h) when EHR technology is in use. (ii) The date and time must be recorded in accordance with the tandard specified at § 170.210(g). (e)(2) (i) The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at § 170.210(h) when the audit log status is changed. (ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g). (e)(3)The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at § 170.210(h) when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at § 170.210(g). (g) Synchronized clocks. The date and time recorded utilize a system clock that has been synchronized following (RFC 1305) Network Time Protocol, (incorporated by reference in § 170.299) or (RFC 5905) Network Time Protocol Version 4, (incorporated by reference in § 170.299). (h) Audit log content. ASTM E2147-01 (Reapproved 2009), (incorporated by reference in § 170.299).

Reference Links	http://healthcaresecprivacy.blogspot.in/2012/09/meaningful-use-stage-2-audit-logging.html
Status	Pending

Note:
Status 'Y': stands for forms/fields that are already available with current patient portal
Status 'N' : for those are not available
Status 'NA': Not applicable

Table 1: Common MU Data Set

Common MU Data Set	Consolidated CDA Template	Status	Patient Portal Page
Patient Name	General Header	Y	Profile/Who
Sex	General Header	Y	Profile/Who
Date of Birth	General Header	Y	Profile/Who
Race	General Header	Y	Profile/Stats
Ethnicity	General Header	Y	Profile/Stats
Preferred language	General Header	Y	Profile/Stats
Smoking Status	Social History Section Smoking Status Observation Entry	Y	
Problems	Problem Section	Y	Med records/ CCR/Problems
Medication List	Medications (entries required) Section Hospital Discharge Medications Section	Y	Med records/ CCR/Medications
Medication Allergies	Allergies (entries required) Section	Y	Med records/ CCR/Alerts
Laboratory test(s)	Plan of Care Section Plan of Care Activity Observation Entry	Y	Med records/ CCR/Results from procedures
Laboratory value(s)/result(s)	Results (entries required) Section	Y	Med records/ CCR/Results from procedures
Vital signs – height, weight, blood pressure, BMI	Vital Signs Section	Y	

Care plan field(s), including goals and instructions	Plan of Care Section	N	
Procedures	Procedures (entries required) Section	Y	Med records/ CCR/Results from procedures
Care team member(s)	General Header	Y	Profile/Choices

Table2: Ambulatory or Inpatient Summary

Data Requirements	Consolidated CDA Template	Status	Patient Portal Page
Dates and Location of Admission and Discharge- Inpatient Only	General Header	NA	
Discharge Instructions- Inpatient Only	Hospital Discharge Instructions Section	NA	
Provider Name and Office Contact Information- Ambulatory Only	General Header	Y	Profile/Choices
Reason for Hospitalization- Inpatient Only	Reason for Visit and/or Chief Complaint Section(s)	NA	