2015 Edition Final Rule: Supporting Care Across the Continuum

Rule Reference: 2015 Edition Health Information Technology (Health IT) Certification Criteria, Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications Final Rule (The "2015 Edition")

Background

The 2015 Edition final rule, published by the Office of the National Coordinator for Health Information Technology (ONC), updates the ONC Health IT Certification Program to make it more open and accessible to other types of health IT and settings beyond those eligible for the EHR Incentive Programs, such as long-term and post-acute care (LTPAC), behavioral health, and pediatric settings. These modifications also are designed to support use of the ONC Health IT Certification Program by other HHS programs and by private entities and associations.

Through the ONC Health IT Certification Program, providers across the care continuum will have improved access to technical standards that form an essential foundation for interoperability and help ensure that key data is consistently available to the right person, at the right place, and at the right time.

Certification Criteria that Support Settings and Use Cases Across the Care Continuum

Below, we have highlighted several new and revised certification criteria that support settings and use cases across the care continuum. We encourage stakeholders to review all available criteria to determine the criteria that best suit their needs.

- *Transitions of care* – A new "transitions of care" ("ToC") certification criterion will rigorously assess a product's ability to create and receive interoperable Consolidated-Clinical Document Architecture (C-CDA) documents according to C-CDA Release 2.1. Testing and certification will support the ability to exchange electronic health information with health IT certified to the 2014 Edition and the 2015 Edition. The "ToC" criterion also focuses on the ability to send and receive the data specified in the Common Clinical Data Set.

- *Common Clinical Data Set summary record* – The final rule adopted two certification criteria focused on the ability of a Health IT Module to *create (criterion)* and *receive (criterion)* a summary care record formatted according to certain C-CDA 2.1 document templates and the Common Clinical Data Set, without testing or certifying to transport standards. These criteria may provide value and increase flexibility for health IT developers who design technology for other programs and settings outside of the EHR Incentive Programs. For example, existing CMS programs point to the use of technology certified to create C-CDA documents with the Common Clinical Data Set, including the requirements providers must meet to furnish chronic care management services, as defined in the CY 2015 Physician Fee Schedule final rule (79 FR 67727). CMS programs also encourage the use of certified health IT for various settings and purposes.

- *"Common MU Data Set" definition/name change* – The final rule changed the Common MU Data Set name to the "Common Clinical Data Set." This aligns with making the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. Equally important, the Common Clinical Data Set includes new and updated standards and code sets for certification to the 2015 Edition. This will support more structured exchange of, and access to, electronic health information.

- *Care plan* – This final rule has adopted a new 2015 Edition "care plan" certification criterion that would require a Health IT Module to enable a user to record, change, access, create, and receive care plan information in accordance with the Care Plan document template in the *HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes*. The data that can be included in the care plan document template can help improve coordination of care by providing a structured format for documenting information such as goals, health concerns, health status evaluations, and interventions. Inclusion of this information is essential to incorporating the patient's perspective, improving outcomes, and represents an important step toward realizing a longitudinal, dynamic, shared care plan.

- *Privacy and security* – The 2015 Edition has adopted a new, streamlined approach to privacy and security certification requirements for Health IT Modules certified to the

2015 Edition. In sum, the privacy and security certification criteria applicable to a Health IT Module presented for certification is based on the other capabilities included in the Health IT Module and for which certification is sought. Under the 2015 Edition privacy and security certification framework, a health IT developer will know exactly what it needs to do in order to get its Health IT Module certified and a purchaser of a Health IT Module will know exactly what privacy and security functionality against which the Health IT Module had to be tested in order to be certified.

- *Exchange of sensitive health information: Data Segmentation for Privacy (DS4P)* – In consideration of stakeholder feedback and several of HHS' overarching policy goals (enabling interoperability, supporting delivery system reform, reducing health disparities, and supporting privacy compliance), the 2015 Edition includes two new certification criteria that incorporate the DS4P standard:

    - *DS4P send* – This criterion enables a user to create a summary record formatted in accordance with the DS4P standard that is document-level tagged as restricted and subject to restrictions on redisclosure.

    - *DS4P receive* – This criterion enables a user to receive a summary record that has been tagged with document-level tags using the DS4P standard. Additionally, a user will be allowed to sequester the document from other documents received and view the restricted document.

  This functionality allows for isolation of parts of the record and can be used to separate and transmit sensitive information that requires special protections. For additional information on the DS4P provisions of the final rule, see *2015 Edition Final Rule*: *Data Segmentation for Privacy (DS4P)* on healthIT.gov.