The Office of the National Coordinator for
Health Information Technology

2015 Edition Final Rule: Data Segmentation for Privacy (DS4P)

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 continue to support the EHR Incentive Programs and to make it more open and accessible to other types of health IT and settings beyond 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.

Data Segmentation for Privacy

The final rule is a critical step forward in enabling individuals with sensitive health conditions to be able to receive the best care possible. Sensitive health information includes conditions and related treatment data that receive special protection under certain laws beyond the protection afforded to all electronic health information under HIPAA. An example of sensitive health information is substance use treatment information protected under 42 CFR Part 2.

As health IT adoption continues to grow, sensitive health data is all too often exchanged via fax or paper-based methods, or excluded from data exchange altogether, meaning a healthcare provider may not have all the relevant data at the point of care. This can lead to lower quality of care for the patient and can also lead to redundant, unnecessary, or harmful care. The final rule addresses the exchange of sensitive information by providing for the certification of health IT to the Data Segmentation for Privacy (DS4P) standard (HL7 Implementation Guide: Data Segmentation for Privacy, Release 1).

The DS4P standard allows a provider to tag a Consolidated-Clinical Document Architecture (C-CDA) document with privacy metadata that expresses the data classification and possible re-disclosure restrictions placed on the data by applicable law. This aids in the electronic exchange of this type of health information. For example, Part 2 requires a patient's consent for a substance use provider to disclose information to another provider. When the patient provides that consent, the information can be tagged in its electronic state as both permissibly disclosed and restricted from further re-disclosure. This means the receiving provider has a more complete picture of the patient through the electronic data. This standard improves patient safety, the comprehensiveness of treatment, and quality of care and support and enables the delivery of more effective care to sub-groups of underserved patients.

Highlights

While the DS4P standard, as fully balloted by HL7, allows for metadata tagging at the document, section, or clinical element level, a Health IT Module will only have to support document-level tagging to be certified to the adopted certification criteria. This supports our goal of ensuring there is a glide path to increasing options to safeguard patient data.

The two certification criteria that incorporate the DS4P standard are:

- *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.