(DS4P) Data Segmentation for Privacy

- **The DS4P HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 was approved in January 2014 as Normative HL7 Standard.**

What is Data Segmentation?

The term “data segmentation” refers to the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization, or individual as being undesirable to share. This basic definition, however, does not account for the multiple permutations of segmentation in the health care context (*i.e.*, granularity), nor does it adequately capture the varied considerations required for development of segmentation policy.

Challenge

Enable the implementation and management of disclosure policies that originate from the patient, the law, or an organization, in an interoperable manner within an electronic health information exchange environment, so that individually identifiable health information may be appropriately shared for: 1) Patient treatment and care coordination; 2) Third party payment; 3) Analysis and reporting for operations, utilization, access quality and outcomes; 4) Public health reporting; 5) Population health, technology assessment and research

Purpose and Goals

The purpose of this initiative is to enable the implementation and management of varying disclosure policies in an electronic health information exchange environment in an interoperable manner with the goal to produce a pilot project allowing providers to share portions of an electronic medical record while not sharing others, such as information related to substance abuse treatment, which is given heightened protection under the law.

Scope

This initiative will focus on defining the use case, its user stories and requirements supporting a standards-based privacy protection architecture and specifically application of data segmentation for interchange across systems. Together with recommendations from the HITSC, the requirements will serve as the basis for a reference model validating the completeness of the standards in fulfilling the defined requirements and maintaining the privacy of the patient data based on patient consent decisions, applicable law and policies. Initial use case functional and data set requirements will encompass metadata tagging of privacy attributes in clinical and policy records and specifically considerations for 42 CFR Part 2 and non-disclosure to payers of patients paying out-of-pocket for their care as defined in Proposed Rule 45 CFR Part 164.522(a)(1)(iv) Existing relevant standards, implementation guides, prototypes and technologies will be looked to when developing the reference model.