Segmenting Data Privacy: Cross-industry Initiative Aims to Piece Out Privacy Within the Health Record

By Johnathan Coleman, CISSP, CISM, CBRM, CRISC

Not all protected health information (PHI) is created equally. Some health data requires special handling according to law, organizational policies, or patient preferences. For appropriate sharing of health information to occur, a patient must trust that a provider organization will properly handle their health data, and disclosing organizations must have confidence that recipients will follow privacy protections according to any special handling instructions. These instructions could be as broad as "opt in/out of sharing" or conceivably as granular as "only share substance abuse information with Doctor X." In order to facilitate this secure and trusted exchange, data needs to be segmented and assigned specific privacy controls.

Data segmentation is "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," according to authors Melissa Goldstein and Alison Rein, who wrote EHR data segmentation policy considerations and analysis for the Office of the National Coordinator for Health IT (ONC). Some healthcare information requires special handling beyond the protections already provided through HIPAA. Additional protection using data segmentation emerged in part through privacy laws that address social hostility and stigma associated with certain medical conditions.

Examples of heightened privacy requirements include the Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (42 CFR part 2), and the laws protecting certain types of health data coming from covered Department of Veterans Affairs facilities and programs (38 USC § 7332). Other laws protect certain categories of data, such as data regarding minors, intimate partner/sexual violence, genetic information, and HIV-related information. In addition, there is a proposed federal rule (45 CFR Part 164.522(a)(1)(iv)) included in the HITECH Act HIPAA modifications that would allow patients to withhold any health information from payers for services that they received and paid for out-of-pocket. Data segmentation would allow healthcare providers to better follow these privacy laws and disclosure policies.

While data segmentation capabilities have not been widely implemented in the US, work is being done to bring privacy metadata standards to the general healthcare public. ONC launched an initiative in 2012 to work on sending and receiving health information segmented using privacy metadata tags.

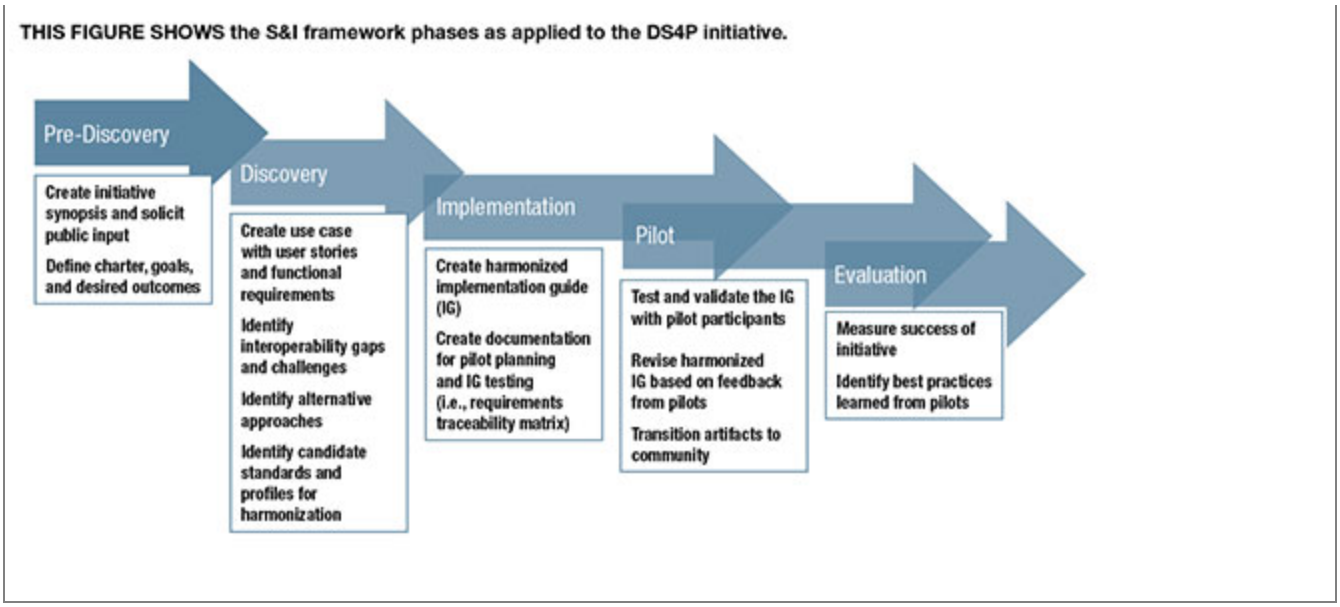
ONC Pilot Tackles Data Segmentation

The Data Segmentation for Privacy (DS4P) initiative utilized ONC's Standards and Interoperability (S&I) Framework as the methodology to address some of these challenges. Over 150 participants from over 50 organizations collaborated to explore the data segmentation challenge.

This initiative included a landscape survey to identify current implementations and validate the business need for data segmentation among stakeholders. A use case document described real-world scenarios, and standards were analyzed using criteria such as standards maturity and compatibility with "meaningful use" EHR Incentive Program requirements.

An implementation guide (IG) documented implementation considerations for standards-based privacy metadata and a reference implementation/pilot phase tested the validity of the guide, documenting test results in a detailed "Requirements Traceability Matrix." A graphical representation of the S&I Framework as applied to the DS4P initiative is shown below in "Figure 1."

Figure 1



The key objectives and results from each of the S&I Framework phases for the segmentation initiative were:

Pre-Discovery: A draft initiative charter was developed for review and approval prior to the full launch of the initiative and call for participation. The launch took place with a community-facing webinar presentation and discussion. Speakers included Melissa M. Goldstein, JD, associate professor in the department of health policy at George Washington University Medical Center, and Joy Pritts, JD, the chief privacy officer at ONC.

Discovery: The purpose of the discovery phase was to identify the use cases and user stories for the initiative. The information and lessons learned through the discovery phase were used to initiate the harmonization process and evaluate viability of the initiative as a candidate for reference implementation/pilot testing. The use case document received public comment and refinement before being unanimously approved by the DS4P community.

Implementation: The implementation phase defined the specifications required to solve the initiative challenge and provide the necessary documentation to plan for operational pilot testing. Three Tiger Teams were formed to address various aspects of the use case-Consent Management Transactions, Information Interchange, and System Requirements. Standards evaluation criteria were developed and candidate standards were assessed against the evaluation criteria, driving the selection of certain standards for inclusion in the Data Segmentation for Privacy Implementation Guide. This proposed approach was presented to ONC's Health IT Standards Committee's Privacy and Security (HITSC) Work Group as a means to gather stakeholder and expert feedback on the concepts articulated in the implementation guide. The initiative also provided a summary of the community analysis of the HITSC recommendations for the use of privacy metadata. The implementation guide was updated based on this feedback and subsequently received majority approval from the DS4P community.

Pilot: The purpose of the reference implementation/pilot testing phase was to test the implementation guide in a realistic setting, including prototype deployments and production deployments to serve as reference. DS4P adopted three pilot ecosystems. The first included the Department of Veterans Affairs (VA) and Substance Abuse and Mental Health Services Administration (SAMHSA) pilot, with participation from MITRE, Jericho Systems, and HIPAAT. The second included the Software and Technology Vendors' Association (SATVA) with participation from Anasazi Software, Valley Hope Association, and Defran. The third pilot ecosystem, Netsmart, focused on the exchange of sensitive data between behavioral health and physical health providers.

Each pilot used portions of the implementation guide that were conducive to their corresponding architectures, and completed a comprehensive requirements traceability matrix to validate which conformance statements from the guide had been tested. This also documented the results. The VA/SAMHSA pilot demonstrated successful data segmentation for portions of the implementation guide at an HL7 conference in Baltimore, MD. The SATVA pilot successfully demonstrated data segmentation during a full meeting of the DS4P community.

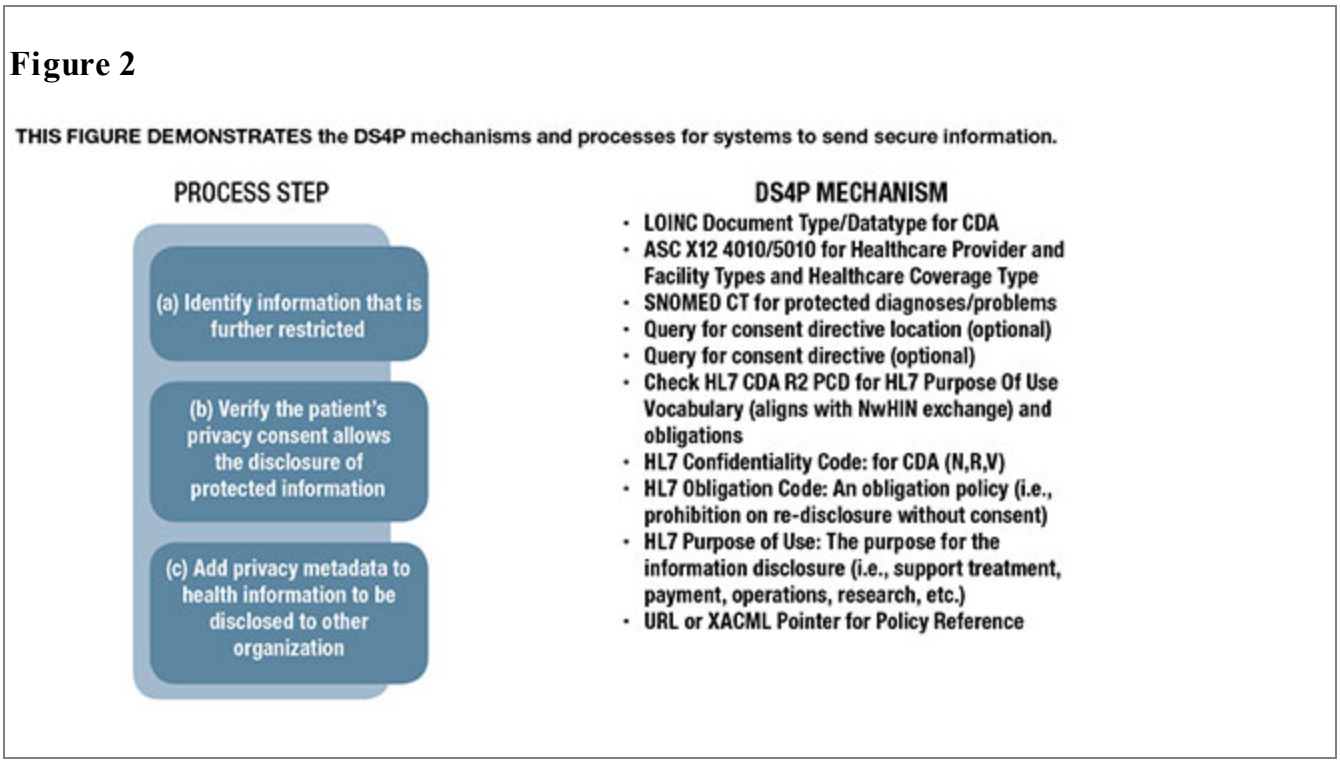
Determining a Recommended Technical Approach

The technical approaches for DS4P differ depending on the underlying transport and associated architecture. In general, the different approaches align in that they rely on certain actions being taken by both the sending system and the receiving system. The sending system must:

1. Identify information that requires enhanced protection or is subject to further restrictions
2. Verify that the patient's privacy consent allows for the disclosure of protected information
3. Add privacy metadata to the health information that is being disclosed

In turn, the receiving system must be able to process the privacy metadata associated with the received health information. If the receiving system has a need to re-disclose the information, it must verify the patient's consent before re-disclosure. The diagram in "Figure 2" below shows some of the possible data segmentation mechanisms that may be used to accomplish these requirements.

Figure 2



In general, the DS4P approach utilizes metadata applied in layers, with each layer of metadata being less revealing as the distance from the clinical payload increases. In addition, a "high watermark" principle is utilized to ensure the highest level of confidentiality code or other restriction that is applied to the clinical data also applies to the entire information exchange associated with that data. For example, where a CDA is used as the clinical payload for a transaction, the document header and document section may include confidentiality codes. In such instances, the confidentiality code of the document header should reflect the most restrictive code used within any of the document sections.

The DS4P community focused on the use of existing and evolving standards to support the need for segmentation of patient data in multiple architectures, including use of SMTP and S/MIME through the Direct Project (with additional IHE XDR support) and use of SOAP architectures that support Integrating the Healthcare Enterprise (IHE) XD* metadata. Furthermore, RESTful approaches are intended to be supported as standards continue to evolve and pilots implement DS4P capabilities in different architectures.

The DS4P community also recognized different approaches for conveying obligations, such as a prohibition on re-disclosure. Understanding the constraints different architectures impose on possible solutions, the DS4P pilots demonstrated how obligations can be implemented through external references and also by using XD* metadata.

Segmentation Enables Private Data Exchange

Data segmentation provides a potential means of protecting specific elements of health information, both within an EHR and in broader electronic exchange environments. Segmentation helps implement current legal requirements and helps honor patient choice.

By executing the various phases of the S&I Framework, DS4P has shown that standards can be used to apply privacy metadata at various layers of an information exchange using structured documents (document entry, document header, envelope, and transport) in order to restrict the flow of certain information while allowing others to flow more freely. DS4P has shown that standards can be used to ensure semantic interoperability for the application and enforcement of obligations or restrictions when handling data across organizational boundaries.

While there is still work to be done in refining approaches to achieving data segmentation, this initiative shows that existing standards and prescriptive EHR system behavior can be used to implement a DS4P capability. It is expected that extensions to existing standards and the adoption of new, emerging standards, such as the HL7 Patient Consent Directive DSTU and the draft HL7 Classification Scheme, will ultimately lead to less complex and more elegant implementations.

The community reached several important conclusions during the DS4P pilot. It recommended standards for privacy and application of privacy metadata at different transaction layers. The initiative successfully demonstrated pilot testing of interoperable privacy protection prototypes compliant with federal privacy and security rules.

The DS4P initiative addressed standards needed to protect those parts of a medical record deemed especially sensitive, or that may otherwise require additional privacy protection, while allowing other health information to flow more freely. Participants hope results from the pilot implementations will encourage broader adoption of data segmentation techniques to enable interoperable implementation and management of varying disclosure policies in an electronic health information exchange environment. This would allow providers to share specified portions of an electronic medical record while retaining others.

References

Goldstein, Melissa M. and Alison L. Rein. “Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis.” Office of the National Coordinator for Health IT. September 29, 2010. http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_950146_0_0_18/gwu-data-segmentation-final-cover-letter.pdf.

Substance Abuse and Mental Health Services Administration. “The confidentiality of alcohol and drug abuse; Patient records regulation and the HIPAA privacy rule; Implications for alcohol and substance abuse programs.” HHS. June 2004. http://www.samhsa.gov/healthprivacy/docs/samhsapart2-hipaacomparison2004.pdf.

Johnathan Coleman (jc@securityrs.com) is principal at Security Risk Solutions, Inc., based in Mt. Pleasant, SC.

Article citation:
Coleman, Johnathan. "Segmenting Data Privacy: Cross-industry Initiative Aims to Piece Out Privacy Within the Health Record" *Journal of AHIMA* 84, no.2 (February 2013): 34-38.