Protecting High-Stakes PHI: DS4P Healthcare Standards Enhance the Privacy of Sensitive Data

Save to myBoK

By Johnathan Coleman, CISSP, CISM, CBRM, CRISC

Sensitive health information is not a rarity in the United States by any means, according to a recent *Issue Brief* published by the Office of the National Coordinator for Health IT (ONC).[1] In the brief, ONC estimated 26 percent of Americans age 18 and older are living with a mental health disorder in any given year, and 46 percent will have a mental health disorder over the course of their lifetime. Patients suffering from serious mental illness have increased rates of co-occurring conditions that will land them in healthcare waiting rooms, which results in a reduced life expectancy of eight to 17 years. When it comes to substance abuse, an estimated eight percent of Americans are in need of drug or alcohol abuse treatment.

The article "Segmenting Data Privacy" published in the February 2013 *Journal of AHIMA* described efforts underway to apply special handling instructions to parts of an electronic health record (EHR) so that extra-sensitive information, like mental health and substance abuse records, can be appropriately shared without unnecessarily compromising the privacy of the individual. In some cases, US law already requires additional protection for information that goes beyond the protections provided through the HIPAA Privacy Rule, such as the Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations [42 CFR Part 2], the confidentiality of certain medical records for Department of Veterans Affairs facilities and programs [38 U.S. Code §7332], and an individual's rights to request privacy protection for protected health information [CFR §164.522(a)(1)(iv) and (vi)].

The Data Segmentation for Privacy (DS4P) Initiative created by the Standards and Interoperability (S&I) Framework defined use cases based around these regulations—all of which are examples of specific privacy policies that can be electronically supported through data segmentation techniques. The regulations were recognized as being broadly applicable in the US, yet specific enough to be addressed through standards harmonization processes within the S&I Framework. It was also anticipated that organizations would be able to leverage the results of the S&I activities to apply similar techniques and principles to help enable implementation of the wider set of privacy policies that currently exist in other healthcare settings.

But the work described in the February 2013 article was just the start. Recent progress in the development of technical standards that support interoperability and introduce additional use cases are being explored by DS4P pilots and cross-industry groups. The work, if widely implemented, could go a long way in better protecting sensitive health information at a time when data breaches are increasing.

Ongoing Standards Development Activities

The S&I DS4P Initiative addressed the challenge of identifying how standards might be used to ensure that EHR systems can apply privacy annotations to data in a way that will be consistently recognized and adhered to by receiving systems. Among the artifacts developed by the community of over 340 registered participants (including committed members from over 100 different organizations) are the DS4P Use Case document and the DS4P Implementation Guide. The S&I Implementation Guide provided a point-in-time reference for DS4P pilots to utilize, but lacked the necessary governance processes utilized by standards organizations to ensure technical specifications can be maintained over time, or formally deprecated when no longer useful. For these reasons, the DS4P S&I community worked closely with Health Level Seven International (HL7) and Integrating the Healthcare Enterprise (IHE) to adopt, mature, and maintain the technical concepts described in the S&I DS4P Implementation Guide.

HL7 is a not-for-profit, ANSI-accredited standards developing organization, and IHE is an initiative led by healthcare professionals and industry representatives that promotes the coordinated use of established standards—such as those developed by HL7—to address specific clinical needs in support of optimal patient care. Both organizations participated in creating a sustainable set of technical specifications which describe how disparate healthcare organizations can apply privacy tags to healthcare data, with the assurance that any obligations, such as "do not redisclose without consent," will be enforced by those who they share the information with.

The following paragraphs summarize the technical work being addressed by IHE and HL7, which collectively can be used to provide a more complete DS4P technical capability.

HL7 Technical Work

At a joint meeting of the HL7 Security Work Group and the HL7 Community Based Collaborative Care (CBCC) Work Group in May 2013, HL7 agreed to adopt and refine the S&I DS4P Implementation Guide as a work item related to the HL7 Healthcare Classification Scheme. During the course of the year, the Security Work Group met regularly to develop a formal standard for DS4P. The standard, "HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1" was developed and first balloted in September 2013 before being finally balloted as a "normative" standard in January 2014. The standard includes three chapters: Chapter 1 is the CDA R2 and Privacy Metadata Content Profile, Chapter 2 is the NwHIN DIRECT Transport Profile, and Chapter 3 is the NwHIN Exchange Transport Profile for DS4P.

IHE Technical Work

A number of work items were proposed by ONC and the S&I DS4P community to IHE. Specifically, two changes to existing IHE specifications and one new project were proposed and accepted. The first change proposal was a straightforward request to include the e-mail address for the author and intended recipient of the clinical document. This enhancement was already being addressed internally at IHE and was recently approved as part of the IHE IT Infrastructure (ITI) Technical Framework (TF) v10 release.

The second change proposal submitted to IHE was an enhancement to the Cross-Enterprise Document Sharing (XDS) profile. The change proposal is intended to describe how security/privacy tags can be included in document sharing metadata. The proposal recommends the addition of three metadata elements (Purpose of use code, Refrain policy code, and Obligation policy code) in addition to "ConfidentialityCode" to support the needs of EHR systems to exchange protected data. It also recommended the permitted values for the ConfidentialityCode be constrained to a simple and more interoperable value set. The XDS metadata change proposal (#690) passed committee review in December 2013 and will appear in a formal change proposal ballot before it is considered final.[2] The concept of security/privacy tags has been developed in HL7 as the "Healthcare Classification System," which is specific to privacy and security classifications.

The new project proposed to IHE was to collaboratively—between IHE, S&I, and HL7—develop a DS4P Implementation Guide that describes how privacy metadata at the transport layer can be applied in a Representational State Transfer (REST) web services environment. After several committee reviews, it was decided by IHE to first develop a new ITI Volume 4 (US realm) section of the Technical Framework for DS4P, and to address REST at a later date. It is anticipated that the proposed project, when complete, will result in the first US realm supplement for ITI and will use conformance language consistent with those described by HL7 for DS4P implementations in the eHealth Exchange (formerly NwHIN) environment, a federally developed health information exchange protocol.

Ultimately a suite of standards are needed for interoperable implementation of DS4P capabilities across organizational boundaries. The Overarching HL7 Standard for DS4P describes which supporting standards are needed, depending on the type of architecture/transport infrastructure being used for the transactions. Table 1 below contains the core set of vocabulary and metadata standards needed to implement DS4P. Table 2 below lists some of the supporting standards for transport, identity, and conveying patient consent directives.

Other Potential Uses of the DS4P Standards

In late 2011, the Institute of Medicine (IOM) issued the report "Incorporating Occupational Information in Electronic Health Records."[3] One of the issues raised by the IOM committee was the challenge posed by EHRs to the privacy and security of various types of records, and the ethical issues specific to occupational health services that need to be reflected in the structure and function of electronic systems.

The implementation of EHR systems creates potential problems related to inappropriate access to personal health records, storage and retrieval of information in relation to fitness-for-work evaluations, insurance coverage for conditions potentially labeled as "work-related," and provision of specific types of information for workers' compensation purposes or for OSHA, among others. The committee noted that new standards for health information exchange are being developed and do not yet address occupational health information.

In parallel, the National Institute for Occupational Safety and Health (NIOSH) at the Centers for Disease Control and Prevention (CDC) has been working to ensure that EHRs improve the clinical care and public health surveillance of workers for both non-work-related and work-related conditions. In June 2013 NIOSH convened a workshop to assess ethical and privacy challenges associated with managing information in EHRs in the context of occupational health. The workshop discussed various use cases, including those associated with segmenting sensitive or non-work-related health information from a work-related claim. Legal, ethical, and technical protections were assessed and strategies such as DS4P were discussed as potential techniques to help ensure that information flows appropriately to the right stakeholders.

Table 1: Core DS4P Vocabulary and Metadata Standards

Below are core vocabulary and metadata standards from the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, which includes Content Profile, Profile for Direct, and Profile for Exchange protocol.

Capability	**Standard/Profile**	**Specific Usage**
Convey Transport Privacy Metadata	Document Exchange Metadata (IHE ITI TF Vol. 3) Profile for Exchange and Direct Metadata	Specifies privacy annotations using the IHE Document Exchange Metadata specification (XDS)
Convey C-CDA Document Privacy Metadata	HL7 Implementation Guide for CDA R2: IHE Health Story Consolidation, DSTU Release 1.1 (US Realm)	Specifies privacy annotations in the body of Consolidated CDA documents
Metadata Vocabularies (for Transport and/or Document Metadata)	HL7 RefrainPolicy	Conveys specific prohibitions on the use of disclosed health information (i.e., prohibition of redisclosure without consent)
	HL7 PurposeofUse	Conveys the purpose of the disclosure of health information (i.e., treatment, research, emergency)
	HL7 BasicConfidentialityCodeKind	Used to represent confidentiality codes associated with disclosed health information (i.e., restricted)
	HL7 ObligationCode	Used to convey specific obligations associated with disclosed health information (i.e., encryption)

	HL7 ActPolicyType	Used to convey a type of policy
	HL7 SensitivityPrivacyPolicy	Used to convey the sensitivity level of a specific policy
	ASC X12 (5010)	Used to define type of insurance coverage
	Healthcare Facility Type Value Set (as defined in HITSP C80)	Subset of SNOMED CT codes to define facility types (and used by systems to determine protected facilities)

Increased Transparency for Consumer Access to Health Information

One of the six S&I DS4P Pilots, the “Jericho Systems/University of Texas Pilot,” was built on the ONC S&I DS4P Use Case to explore mechanisms that support:

- Increased record integrity through patients’ reports of unexpected requests for a patient’s consent directive (i.e., miscorrelations)
- Increased identification of medical fraud and waste through patient identification of suspicious requests for their PHI
- Increased participation in the sharing of EHR records through trust fostered by involving patients in the sharing of their records

While these goals were not described in the S&I DS4P Initiative Charter, the pilot utilized the ONC DS4P Use Case as the basis for exploring their additional goals. In this context, the pilot utilized an external patient consent repository to provide machine-readable consent directives that can be processed according to various privacy policies as part of any automated release of protected health information (PHI) on the eHealth Exchange. A standard audit record documenting the resulting release decision to the consent repository was used to provide capabilities for future patient review.

The pilot used standards-based message formats, consistent with current healthcare standards, to support fine-grained patient consent over released PHI, including segmented data. The resulting “reference implementation” was successfully tested by an academic institution, a healthcare provider system, and a security software vendor.

Apparent Benefit to the International Community

The challenges associated with the special handling of extra-sensitive healthcare information are not unique to the United States. For example, in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs healthcare-related information handling practices. This federal act provides privacy protection for healthcare-related information in the private sector throughout Canada, except for instances where a province already has legislation declared “substantially similar” to the act. Currently six out of the 10 provinces have substantially similar legislation.

PIPEDA requires consent of the individual for collection, use, or disclosure with some exceptions, such as research or risk of serious bodily harm. The mechanism for obtaining consent is not specified, but it recommends that express consent be used for more sensitive information. As another example, Ontario’s healthcare privacy legislation, the Personal Health Information Protection Act (PHIPA), established what is commonly referred to as the “lock-box provision.”[4] This requires healthcare providers to be able to “lock up” any segment of PHI from any individual at the request of a patient.

For example, a patient can request that only their mental health team ever be able to see any of their PHI that relates to mental health or addictions, including diagnoses, medications, and treatments, and that this data be segmented away from all other providers. Similarly, a patient can also request that a given provider or providers be restricted from seeing any or just a segment of their PHI. This legislation came into effect in Ontario in 2004, and all healthcare providers in Ontario have been subject to it since November 1, 2005.

To date, few technical implementations have addressed the lock-box provision. As is the case in the US, most organizations comply with this requirement manually. For example, if a patient provides an express consent directive, their information is simply not entered into the EHR and is kept on paper in order to ensure that disclosures of their records are tightly controlled.

In Europe, countries also face the realities of adjudicating and enforcing privacy laws across jurisdictional boundaries. Recent collaborations between Switzerland, Austria, and Germany further demonstrate substantial interest and growing needs for effective privacy protection at the lowest feasible level of granularity, whether that be at the document level, or individual entries within a structured clinical document. DS4P can provide that granular protection.

Table 2: Supporting Standards Referenced or Utilized by DS4P

Supporting Data Segmentation for Privacy (DS4P) standards, which are referenced in the DS4P Implementation Guide, are listed below.

Capability	**Standard/Profile**	**Specific Usage**
Transport	SOAP	Transport-level security
	SMTP and S/MIME	S/MIME attributes are bound to SMTP to provide for the use of secure e-mail as the transport mechanism for exchanging patient data
Conveying Identity	Cross-Enterprise User Assertion (XUA) OASIS SAML Specification V 2.0	IHE XUA Metadata SAML Assertion (SAML Request and Response)
	X.509 Digital Certificates	PKI to support Direct implementations
Patient Consent Structure	HL7 Implementation Guide for CDA, Release 2: Consent Directives, Release 1 (DSTU)	Provides representations for expressing privacy preferences and exchanging privacy policies that can be enforced by consuming systems

Future Bright for DS4P

Vendors are starting to integrate DS4P work into their products. At the 2014 HIMSS Conference in February, a major EHR vendor demonstrated sending tagged data using DIRECT health information exchange protocol. This demonstration built on capabilities developed and tested by the former SATVA DS4P pilot of the S&I Framework, and the expectations are that the functionality will be in production during 2014.

New projects and further refinements to DS4P specifications are being discussed in various communities, including the DS4P pilots and International Standards Organizations. Examples include updates to standards which inform DS4P activities and/or artifacts, including the HL7 CDA Consent Directive Implementation Guide, HL7 Behavioral Health CDA Implementation Guide, and HL7 Healthcare Classification System. Pilot activities with HL7's Fast Healthcare Interoperability Resources (FHIR) show promise for rapid implementation of DS4P, as demonstrated at the HL7 FHIR Connect-a-thon held in January 2014.

As the HL7 Healthcare Classification System gains more US and international recognition, and pilots continue to broaden their sophistication, such as the SAMHSA Consent-2-Share project, additional capabilities and concepts like "data-provenance" may increase the fidelity of what is considered reasonable for EHR systems to achieve when protecting sensitive health information.

Acknowledgements

David Staggs, JD, with Jericho Systems, and Mike Davis with the Department of Veterans Affairs contributed to various sections of this article.

Notes

1. Williams, Aja B. "Behavioral Health and Health IT." *ONC Issue Brief*. September 26, 2013. http://www.healthit.gov/sites/default/files/bhandhit_issue_brief.pdf.
2. IHE Change Proposal. "CP-ITI-690-05." December 5, 2013. ftp://ftp.ihe.net/IT_Infrastructure/TF_Maintenance-2014/CPs/Ballots/ballot-20/.
3. Institute of Medicine. "Incorporating Occupational Information in Electronic Health Records: Letter Report." September 30, 2011. http://www.iom.edu/Reports/2011/Incorporating-Occupational-Information-in-Electronic-Health-Records-Letter-Report.aspx.
4. ServiceOntario. "Personal Health Information Protection Act." 2004. http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm.

Reference

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.

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

Article citation:
Coleman, Johnathan. "Protecting High-Stakes PHI: DS4P Healthcare Standards Enhance the Privacy of Sensitive Data" *Journal of AHIMA* 85, no.4 (April 2014): 30-34.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.