Data Segmentation for Privacy (DS4P) Update

HIMSS 2015

Lucia Savage, JD
Chief Privacy Officer
Data Segmentation for Privacy

NEED FOR DATA SEGMENTATION
The Need for Data Segmentation

• HIPAA Privacy Rule allows health care providers to disclose protected health information without patient consent for treatment, payment and health care operations purposes.

• HIPAA leaves in place other state and federal privacy laws that are more protective.

• Some state and federal privacy laws which address social hostility and stigma associated with certain medical conditions, require consent to disclose information beyond that required by HIPAA. *

Examples of Heightened Legal Privacy Protections

• **42 CFR Part 2**: Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations protect specific health information from exchange without patient consent.

• **Title 38, Section 7332, USC**: Laws protecting certain types of health data coming from covered Department of Veterans Affairs facilities and programs. Types of data include sickle cell anemia, HIV, and substance abuse information.

• **45 CFR §164.522(a)(1)(iv)**: Effective 3/26/2013, this final rule describes how patients may withhold any health information from health plans for services they received and paid for out-of-pocket.*

*Patient, not provider, has responsibility for ensuring that downstream recipients know that patient is requesting restriction.*
Why is this important?

• An estimated 26% of Americans age 18 and older are living with a mental health disorder in any given year.
• 46% of Americans will have a mental health disorder over the course of their lifetime.
• An estimated 8% of Americans are in need of drug or alcohol abuse treatment.
• Patients suffering from serious mental illness have increased rates of co-occurring conditions, which results in a reduced life expectancy of 8-17 years.
• Of 50 states, an estimated 18 states have rules regarding mental health data that are more privacy protective than HIPAA; an estimated 17 states have similar rules that are specific to drug or alcohol abuse (not Part 2 rules)
• CMS CMMI State Innovation Model Round 2 has awarded over $1.2 billion million to states to test and/or implement new models of care delivery, including those that integrate behavioral and physical health.
Data Segmentation for Privacy

“WE HAVE THE TECHNOLOGY...”
AKA “IT’S THE RULES...”
Laws, regulations, and policies for patient consent

Laws, regulations, and policies for sensitive information

Consent models (opt-in, opt-out, with restrictions, etc.)

HIO/HIE Architecture

EHR system interoperability

Consent directive (paper/electronic)

Patient provides consent to share sensitive health information and HIPAA Permitted Uses and Disclosures
Sample State Definitions of Mental Health Information (for Disclosure Purposes)

D.C. Code § 7-1201.01 Definitions

Mental health information means any written, recorded or oral information acquired by a mental health professional in attending a client in a professional capacity which:
(A) Indicates the identity of a client; and
(B) Relates to the diagnosis or treatment of a client’s mental or emotional condition.

N.C. Gen. Stat. § 122C-3 Definitions

Confidential information means any information, whether recorded or not, relating to an individual served by a facility that was received in connection with the performance of any function of the facility. Confidential information does not include statistical information from reports and records or information regarding treatment or services which is shared for training, treatment, habilitation, or monitoring purposes that does not identify clients either directly or by reference to publicly known or available information.
• States philosophically aligned

• State privacy and consent laws are diverse in content

• Diversity in organizational policies within states

• See roadmap appendix A and B for ONC Consent Bibliography
Data Segmentation for Privacy

ABOUT THAT TECHNOLOGY . . .
AKA DATA SEGMENTATION CHALLENGES
DS4P Standards:
What can DS4P do?

- DS4P was tested on substance abuse information (for example, 42 CFR Part 2 data) where the category of special protection derives from the federally funded program where the care is supplied
  - 42 CFR Part 2 (Part 2) is a federal law and does not change across state lines
  - 42 CFR Part 2 protect adheres to care supplied in buildings covered by that regulation and the statute it derives from

- DS4P can therefore recognize that a provider applied special protections because of the physical source of the data;
  - Therefore, segmentation can be based on the whole program, not specific clinical portions of it

For example, in a Part 2 covered program a physician may track a patient’s blood pressure. Although this data might not be specially protected otherwise, it is specially protected because the care is supplied in a Part 2 covered program.
• What about segmentation necessary due to the *clinical nature* of the data (not a location)?

• There are 8 basic categories of special privacy protections due to clinical nature, not necessarily where care was provided
  – HIV/AIDS; Drug/Alcohol Abuse (not Part 2), Mental Health/Behavioral Health; Reproductive Health of Women; Genetic Information (not GINA); STD; Teen Health Information; Domestic Violence health information.

• DS4P might be effective if there was harmonization between legal definitions of what is protected and medical codes (e.g. ICD10).

• Harmony is lacking:
  
  Example: in a PCP office, some collected information is specially protected, such as evidence that a Chlamydia test occurred, while other information is not. All care occurs in the same place.

• Even if a disclosing system segments data, the receiving system may not be able to recognize that segmentation (more later).
• Technical standards can help organizations implement policy, but first the policy must support the use of the technical standards.

• Currently, although state law is philosophically aligned, it is not harmonized, so nationwide mapping to code sets has not taken root.

• Lack of harmony may:
  – Exaggerate privacy concerns because of confusion.
  – Undermine potential business cases for interoperable information exchange.
  – Foster skepticism about the ability of information exchange to deliver comprehensive data.
DS4P Standards: How it Works

Separating Policy from Technical Capability

The DS4P standard enables interoperability and provides a capability to support existing privacy law, including federal, state, and local laws.

The standard uses document level tagging as the mechanism to convey confidentiality levels and obligations, but also specifies how to be more granular (e.g. sections or entries inside the document):

- Depends if the implementing (sending or receiving) system can support it.
Policy Challenges

- Laws tell data-holders not to disclose; law rarely tells them what to say about that non-disclosure. For example:
  - HIV Status: **Redacted**

- This is a likely indicator that the patient has a test result
  - if the applicable law protects results of tests, not occurrences, this may indicate a positive result; or
  - HIV Status: **No data available**

- This is may be misleading for a physician, who may then make a health decision for the patient without knowing important details that could lead to safety issues.
  - HIV Status: [record is silent]

- This is ambiguous. The recipient does not know if there was a redaction, or no data is available.
• **How to Segment:** There are multiple levels at which segmentation could occur, such as:
  – Type of Data category of data - e.g. medications, diagnostic codes, etc.
  – Clinical category of code of whatever type
  – Disclosing provider
  – Intended recipient
  – Program type (e.g. Part 2 clinic)

• **Structured vs unstructured Data:** Prevalence of free-text complicates identification of data that is subject to enhanced protection.
Things to Solve

• **Granularity:** Should data be segmented:
  – At the “whole document” level?
  – For parts of a document?
  – According to clinical nature within the document?

• Standardized mapping of specially protected categories to codes would make segmentation more predictable:
  – For *individuals* through standard understanding
  – For providers through standard expectations
  – For developers, with less confusion about what law requires

• Currently, not every receiving system can understand 42 CFR Part 2 segmented data, i.e., their system does not recognize that it is receiving data that is subject to heightened protections based on Part 2 law.
Data Segmentation for Privacy Initiative

TECHNICAL APPROACH
The Patient receives care at their local hospital for a variety of conditions, including substance abuse as part of an Alcohol/Drug Abuse Treatment Program (ADATP).

Data requiring additional protection and consent directive are captured and recorded. The patient is advised that the protected information will not be shared without their written authorization.
A clinical workflow event triggers additional data to be sent to Provider/Organization 2. This disclosure has been *authorized* by the patient, so the data requiring heightened protection is sent along with a prohibition on redisclosure.

Provider/Organization 2 electronically receives and incorporates patient additionally protected data, data annotations, and prohibition on redisclosure.
Types of Privacy Metadata used by DS4P

• **Confidentiality Codes:**
  – Used by systems to help convey or enforce rules regarding access to data requiring enhanced protection. Uses “highest watermark” approach.

• **Purpose of Use:**
  – Defines the allowed purposes for the disclosure (e.g. Treatment, Emergency Treatment etc).

• **Obligations:**
  – Refrain Codes: Specific obligations being placed on the receiving system (e.g. do not re-disclose without consent)
HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1

- Voted on and approved at the highest level, to become what HL7 calls a “normative” standard, and has also received ANSI (American National Standards Institute) accreditation.

- The standard uses vocabularies to convey specific meanings, such as “Do not re-disclose without consent” or “This document is restricted”.
## STANDARD: HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (Includes Content Profile, Profile for Direct, Profile for exchange)

<table>
<thead>
<tr>
<th>Capability</th>
<th>Standards/Profiles used by the HL7 DS4P R1 Standard</th>
<th>Specific Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata Vocabularies (for Transport and/or Document Metadata)</td>
<td><strong>HL7 RefrainPolicy</strong></td>
<td>Conveys specific prohibitions on the use of disclosed health information (e.g. prohibition of redisclosure without consent)</td>
</tr>
<tr>
<td></td>
<td><strong>HL7 PurposeofUse</strong></td>
<td>Conveys the purpose of the disclosure of health information (e.g. treatment, research, emergency)</td>
</tr>
<tr>
<td></td>
<td><strong>HL7 BasicConfidentialityCodeKind</strong></td>
<td>Used to represent confidentiality codes associated with disclosed health information (e.g. restricted) as specified in the HL7 Healthcare Security Classification standard (HCS).</td>
</tr>
<tr>
<td></td>
<td><strong>HL7 ObligationCode</strong></td>
<td>Used to convey specific obligations associated with disclosed health information (e.g. encryption)</td>
</tr>
<tr>
<td></td>
<td><strong>HL7 ActPolicyType</strong></td>
<td>Used to convey a type of policy</td>
</tr>
<tr>
<td></td>
<td><strong>HL7 SensitivityPrivacyPolicy</strong></td>
<td>Used to convey the sensitivity level of a specific policy</td>
</tr>
</tbody>
</table>
## Other Standards Referenced by the HL7 DS4P Standard:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Standard/Profile</th>
<th>Specific Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Consent Structure</td>
<td>HL7 Implementation Guide for CDA®, Release 2: Consent Directives, Release 1 (DSTU)</td>
<td>Provides representations for expressing privacy preferences and exchanging privacy policies that can be enforced by consuming systems</td>
</tr>
<tr>
<td>Transport</td>
<td>SOAP</td>
<td>Transport-level security</td>
</tr>
<tr>
<td>Transport</td>
<td>SMTP and S/MIME</td>
<td>S/MIME attributes are bound to SMTP to provide for the use of secure email as the transport mechanism for exchanging patient data</td>
</tr>
<tr>
<td>Conveying Identity</td>
<td>- Cross-Enterprise User Assertion (XUA)</td>
<td>IHE XUA Metadata</td>
</tr>
<tr>
<td>Conveying Identity</td>
<td>- OASIS SAML Specification Version 2.0</td>
<td>SAML Assertion (SAML Request and Response)</td>
</tr>
<tr>
<td>Conveying Identity</td>
<td>X.509 Digital Certificates</td>
<td>PKI to support Direct implementations</td>
</tr>
</tbody>
</table>
Variation in rules about permission to access, use or disclose makes it difficult to build software systems that accurately capture, maintain, and persist this data. But we need software systems to capture and persist both written individual directions and what is permitted without a written individual direction.
Data Segmentation for Privacy Initiative

CONCLUSION
Conclusion

• While DS4P can clearly be used, we need to strengthen the standards so that the consent of the patient as required by law can be carried forward.

• The DS4P pilots give optimism. And, at the same time, policy needs to be harmonized to take full advantage of DS4P.

• Improving health outcomes for individuals with complex, comorbid conditions depends on the twin goals of:
  – Efficient, nationwide standards by which individuals can ensure that their specially protected health information flows where they need it to for care.
  – Appropriate standard controls to respect the privacy of individuals who do not want their specially protected data to flow.

• How to achieve goals: See Interoperability Road Map
Data Segmentation for Privacy Initiative

QUESTIONS?