Behavioral Health Data
Privacy and Confidentiality

Ultra-Sensitive Privacy Disclosures
How to comply with a complex regulatory environment.

Presented by the Software and Technology Vendors’ Association

April 2014

John Leipold, DBA, MBA
President/CEO Valley Hope Technology
Board Member, Software and Technology Vendors’ Association
jleipold@valleyhope.com
www.Valleyhope.com
The Software and Technology Vendors’ Association is a trade organization for vendors of behavioral health and human services software and information technology. Its members have a genuine concern for promoting the use of effective information technology in behavioral health and human services; helping to formulate and support quality improvement for the highest industry standards; and facilitating the delivery of more efficient and effective consumer services through use of information technology.

http://www.satva.org/
eHIE is getting a good push...

Recent federal initiatives, for example:

• The American Recovery and Reinvestment Act.
• The Affordable Care Act.

... promote electronic health information exchange (eHIE) as a foundational principle for improving healthcare and reducing costs.

• Electronic HIE presents difficult technology challenges for privacy and confidentiality.
• A complex regulatory environment magnifies these challenges.
A Complex Regulatory World...

SATVA formed its Interoperability Work Group in 2009 and has devoted considerable time and financial resources designing practical methods for exchanging electronic health information in full compliance with a complex regulatory environment.

What we learned:

• The regulatory environment covering the privacy and disclosure of Personal Health Information across the federal government and the 50 states is a minefield of disparate laws and regulatory language but the legal language always references the act of disclosure.
• To communicate clearly and consistently, SATVA refers to these disclosures as *Ultra-Sensitive Privacy Disclosures (USPD)*.
We also learned...

- All the laws and regulations share a common architecture placing obligations on persons or entities who hold ultra-sensitive health information and may have reason to disclose it.
- Common architecture makes it possible to generalize a common model because there is no way to make electronic health information exchange practical addressing each privacy law individually.
- SATVA uses 42 CFR Part 2, the law and regulations providing privacy protections to addiction treatment records, as its demonstration model since 42 CFR Part 2 is about as restrictive as privacy regulations get.

SATVA believes if an EHR can comply with Part 2 then it can comply with other regulatory requirements as well.
Traditional Disclosure Practice...

- Paper consent forms.
- Printed or photocopied patient case records.
- The manual process is inefficient but relatively effective with respect to protecting patient confidentiality.
  - Records are traditionally disclosed based on a human judgment of the regulatory environment for the privacy and confidentiality of personally identifiable health information.
  - The behavioral healthcare provider is the record custodian and is responsible to protect patient privacy and confidentiality within the structure of the regulatory environment.
Protecting Highly Sensitive Health Information...

- Privacy laws are enacted to address stigma and the vulnerabilities that result from stigma.

- Gratuitous disclosure can make persons more vulnerable to adverse outcomes (e.g., loss of employment, insurance denials, legal, law enforcement).
Protecting Highly Sensitive Health Information...

Regulations under CFR 42 Part 2...

- Prohibit the disclosure and use of patient records without patient consent.
- Permit disclosure only when the patient provides written authorization in the form of a properly executed release of information (consent) form.
- Provide for limited exceptions...
  - Medical emergencies (break the glass rule);
  - Qualified service organizations;
  - Program audit and evaluation and for research purposes if no patient identifying information is released;
  - If a crime or threat of a crime has occurred on program premises or against program personnel;
  - Suspected child abuse or neglect; and
  - When a proper court order exists compelling the disclosure. (There are specific court order requirements under 42 CFR Part 2.)
Protecting Highly Sensitive Health Information...

With those severely limited exceptions,

the regulations give the patient control over disclosures...

... and the providers are obligated to respect patients’ wishes...
The Critical Concept...

- Compliance with 42 CFR Part 2 ensures that an alcohol or drug abuse patient is not made more vulnerable by reason of the availability of his or her patient record than an individual who has an alcohol or drug problem and who does not seek treatment.

Many alcohol or drug addicted persons will not seek treatment without confidence their treatment provider will protect the treatment record.
It’s the Disclosure...

• It is the disclosure itself that must comply with the regulatory requirements.

  • The privacy rights and obligations created by Part 2 attach to the entirety of a record created by a federally assisted substance abuse program (a “Part 2 Record”). This includes information that identifies a person as a patient at a substance abuse program as well as any information in the clinical record.

*It’s an important distinction... it’s the act of disclosure that must comply, not the information in the record.*
What’s the Electronic Health Information Exchange Problem?

• Addiction treatment providers can disclose the record only when consent is valid.
  – *Recipient(s) must be named* (unlike HIPAA-level consent which can stipulate any provider or care organization that receives the disclosure).
  – *Effective period of consent cannot be open ended; it must have specific expiration.*

Absent valid consent, a covered substance use treatment provider cannot respond to a record locator service (RLS) query with other than “cannot confirm nor deny...”
Data Segmentation...

• Data Segmentation
  – Focus is on data elements.
    • 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.
  – Requires meta-tags.

The SATVA Ultra-Sensitive Privacy Disclosure (USPD) method provides for data element meta-tagging but 42 CFR Part 2 and other privacy regulations require the entire disclosure is treated as ultra-sensitive. Therefore, the SATVA USPD method simplifies data segmentation by tagging all data elements at the same ultra-sensitive level as the disclosure in its entirety.
Part 2 Compliant Electronic Disclosure

• Application of the (Part 2) rule is based on the source of a record, not on the sensitivity of any of the information included in the record.

• *Part 2 compliant electronic disclosure requires only that the disclosure source and disclosure target share a common understanding of the disclosure.*
SATVA Ultra-Sensitive Privacy Disclosure (USPD)...

• Part 2 Compliant Electronic Disclosure
  - Addresses the act of information disclosure.
  - Requires no infrastructure beyond the standards provided by HL7 and the NwHIN.
The SATVA USPD Method

The SATVA USPD method is based on...

- Functionally that executes using public domain content standards (e.g., HL7, http://www.hl7.org/) and public domain communication standards (e.g., the Nationwide Health Information Network (NwHIN, http://wiki.directproject.org/))
- Compliance with the regulatory environment for privacy and confidentiality including 42 CFR Part 2, the federal law enacted to protect addiction treatment records.
- The SATVA Data Segmentation for Privacy (DS4P) work group pilot project.
  - DS4P is part of the Office of the National Coordinator for Health Information Technology (ONC) Standards and Interoperability (S&I) Framework. The S&I Framework is a collaborative community of participants from the public and private sectors who are focused on providing the tools, services and guidance to facilitate the functional exchange of health information.
Making it work...

• The SATVA method empowers relatively easy consented communication of ultra-sensitive health information between two or more providers that can communicate via the NwHIN Direct open specification or other appropriate, common transport protocol.

• SATVA’s Ultra-Sensitive Privacy Disclosure Implementation Guide (USPD IG) implements a small handful of coded disclosure purpose and recipient obligations derived from the work product of the DS4P work group that are added to Continuity of Care Documents (CCDs) or to the message envelope metadata.

  – These coded obligations convey the intentions and expectations under which patients have signed locally maintained consent documents.
Making it work...

• The SATVA USPD is founded on a few basic principles...
  ✓ The entire record is covered.
  ✓ Privacy notices are conveyed within the metadata transporting the disclosure as well as within the disclosure payload itself.
  ✓ Obligations on the recipient are clearly communicated.
    ✓ The recipient cannot re-disclose without obtaining further written consent from the patient.
    ✓ The recipient can use the disclosure only for specified purposes, e.g., payment, treatment, or operations.
      ✓ The SATVA USPD is extensible but currently supports only the use for “treatment.”
What gets electronically exchanged?

- The **Continuity of Care Document** (CCD) is an electronic document created by an EHR dynamically and on demand.
- A CCD is structured according to standards (HL7).
- A CCD uses common vocabulary ensuring “semantic” interoperability.
- Software systems can “parse” a CCD and incorporate structured data elements directly into an EHR database.
**What’s in a CCD?**

<table>
<thead>
<tr>
<th>Problems</th>
<th>Immunizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedures</td>
<td>Medical equipment</td>
</tr>
<tr>
<td>Family history</td>
<td>Vital signs</td>
</tr>
<tr>
<td>Social history</td>
<td>Functional stats</td>
</tr>
<tr>
<td>Payers</td>
<td>Results</td>
</tr>
<tr>
<td>Advance directives</td>
<td>Encounters</td>
</tr>
<tr>
<td>Alerts</td>
<td>Plan of care</td>
</tr>
<tr>
<td>Medications</td>
<td></td>
</tr>
</tbody>
</table>
Electronic Information Exchange

**PUSH TRANSACTION (Slide 1 of 2)**

- Common transaction type supported by the SATVA USPD method.
- Example: discharge summary sent from a primary care provider to a continuing care provider.
- Continuing care plans are made by the discharging provider and agreed to by the discharging patient.
- Discharging patient authenticates an electronic consent for disclosure. If the provider is a “Part 2 Provider” the consent must comply with all 42 CFR Part 2 requirements.
- The discharging provider’s EHR dynamically assembles discharge summary information and creates a CCD.
- The EHR transmits the CCD to the disclosure target.
Electronic Information Exchange

**PUSH TRANSACTION (Slide 2 of 2)**

- The EHR transmits the CCD to the disclosure target.
- The EHR at the disclosure target location alerts the disclosure target that a CCD has arrived electronically.
- When an authorized user at the disclosure target location attempts to view the CCD the electronic “package” in which the CCD is wrapped alerts the user the “package” contains an ultra-sensitive disclosure of protected health information.
- The user must agree to the obligations:
  - Utilize information ONLY for purposes specified (e.g., treatment).
  - Re-disclosing the information is strictly prohibited.
- Only on agreeing to the obligations will the EHR display the CCD to the user.
Electronic Information Exchange

**PUSH TRANSACTION**

**RESPONSE EXPECTED, RESPONSE PROVIDED, RECORDS DISCLOSED**

- A slightly more complex example also supported by the SATVA USPD method.
- Example: a patient admits at a treatment provider and alerts the provider that there are records of prior treatment at another provider.
- The admitting provider on obtaining the patient’s consent pushes a CCD to the former provider requesting records.
- If the provider receiving the request has compliant consent for the requested disclosure then the receiving provider’s EHR will dynamically create a CCD and push the disclosure back to the requesting provider.
- The requesting provider will need to agree to the obligations on receiving the disclosure.
In this example, a requesting provider sends a former Part 2 provider a request for records. If identity match or compliant consent for disclosure fails validation the former provider is compelled to reply as neither confirming nor denying the former patient exists or that records for the former patient exist.
The SATVA USPD method is extensible to the “break the glass” scenario.

“Break the glass” occurs when medical professionals request records under Part 2’s medical emergency provisions.

A Part 2 program can make disclosures to medical personnel if there is a determination that a medical emergency exists, i.e., there is a situation that poses an immediate threat to the health of any individual and requires immediate medical intervention [42 CFR §2.51(a)].
Although redisclosure during break the glass is permitted Part 2, SATVA recommends recipients are asked to exercise redisclosure permissions only for the duration of the emergency and only as necessary to treat the emergency. After the emergency SATVA believes the Part 2 information should not be further redisclosed.
Thank You...

• More information on interoperability is available from SATVA at [http://www.satva.org/](http://www.satva.org/)

Contact SATVA:
David Jaffe, Executive Director,
Email: info@satva.org
Phone: 646-233-0167.
Mailing Address: SATVA, 347 Fifth Avenue, Suite 703, New York, NY 10016