Health IT Standards Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

Privacy & Security Tiger Team: Update on C/A workgroup recommendations for behavioral health & CEHRT

May 6, 2014

Tiger Team Members

- **Deven McGraw,** Chair, Manatt, Phelps & Phillips, LLP
- **Micky Tripathi,** Co-Chair, Massachusetts eHealth Collaborative
- **Dixie B. Baker,** Member, Martin, Blanck, and Associates
- **Judy Faulkner,** Member, Epic Systems Corporation
- **Leslie Francis,** Member, University of Utah College of Law
- **Larry Garber,** Member, Reliant Medical Group
- **Gayle B. Harrell,** Member, Florida State House of Representatives
- **John Houston,** Member, University of Pittsburgh Medical Center, NCVHS
- **David Kotz,** Member, Dartmouth College
- **David McCallie, Jr.,** Member, Cerner Corporation
- **Wes Rishel,** Member, Gartner, Inc.
- **Stephania Griffin,** Ex Officio, Veterans Health Administration
- **Verne Rinker**, Ex Officio, HHS – Office for Civil Rights
- **Andrea Wilson,** Ex Officio, Veterans Health Administration
- **Kitt Winter,** Member, Social Security Administration

Agenda

- Provide update on Tiger Team discussion on recommendations from Certification & Adoption Workgroup re: certification to enable exchange of behavioral health data
  - Background on the issue
  - Outreach and what we've learned
  - Straw recommendations discussed
  - Results of discussion to date
- Obtain early feedback from the HITPC

New PS TT Topic: Recommendations for ALL Providers*

Enhancements to Privacy and Security

C/A WG requests that the P&S TT examine the proposed areas for certification for ALL providers (MU and non-MU) and provide recommendations to the HITPC:

- Use of the HL7 privacy and security classification system standards to tag records to communicate privacy related obligations with the receiver.
- Standards for controlling re-disclosure of protected data
- ONC should consider supporting equivalent functionality in MU 3 for standards for communicating privacy policies and controlling re-disclosure of protected data.
- Developing consensus on standards for consent management functionality needed by BH providers to comply with diverse federal and state confidentiality laws , including the Data Segmentation for Privacy Standard

Future work: Incorporate granular data segmentation when such standards are available.

*Slide 10 of the Certification/Adoption Workgroup presentation, March 4, 2010 meeting

42 CFR Part 2 (1 of 2)

- Applies to federally assisted, substance abuse treatment programs.
- Patient authorization is required for disclosure of identifiable information from one of these programs (with limited exceptions).
- Such information may not be re-disclosed by the recipient without further patient authorization.

42 CFR Part 2 (2 of 2)

- Similar information provided by an entity that is not a federally assisted, substance abuse program (or by patients themselves), is not subject to Part 2 requirements.
- Similar regulations govern disclosure of other behavioral health/sensitive data (although further “re-disclosure” prohibitions are not typical).

Previous Recommendations of HITPC

- 9/1/2010 transmittal letter:
  - Letter incorporated lessons learned from initial hearing on data segmentation technologies.
  - Technology to support more granular consent is "promising" but still in early stages of development and adoption.
  - This should be a priority for ONC to explore further, through pilots.
  - In the interim, education of both providers and patients, re implications of consent decisions and potential limitations of technology approaches to consent management, is key.

Observations (1)

- 2010 recommendations acknowledged the difficult issues that arise from "granular consent," and those difficulties still exist.
- The need to provide coordinated care for individuals with mental/behavioral health issues is clear.
- Enhanced consent requirements for behavioral health data (in particular, 42 CFR Part 2) were implemented to address reluctance of individuals to seek care for behavioral health conditions.

Observations (2)

- However, the ability of patients to withhold consent to disclose information is of concern for providers.
- Providers want to provide the best care for their patients and have concerns – both out of professional obligation and due to liability concerns – about incomplete ("Swiss cheese") records.
  - Providers needing to act on incomplete information is not necessarily new, but the use of EHRs, especially EHRs that are connected to HIEs or other data networks, may create an expectation of more complete information.

State of Technology – DS4P

- DS4P is an initiative of ONC's S&I Framework to pilot promising technologies for enabling the disclosure of records covered by 42 CFR Part 2 (and potentially other granular consent requirements).
  - Currently 6 Pilots: VA/SAMHSA Pilot, SATVA Pilot, Netsmart Pilot, Jericho/UT Austin Pilot, GNOHIE Pilot, Teradact Pilot
- In light of the initial recommendations of the C/A Workgroup, we sought to understand more about these pilots and actual implementation of DS4P, as well as an understanding of how Part 2 data is handled today by providers and some HIEs.

Who We Talked To

- Jonathan Coleman, Initiative Coordinator for the Data Segmentation for Privacy Initiative at ONC
- Dr. Larry Garber (PSTT Member), Reliant Medical Group
- Matthew Arnheiter, Netsmart Pilot
- Dan Levene, Cerner Pilot
- Laura Young, Behavioral Health Information Network of Arizona
- Kate Tipping and Maureen Boyle, Substance Abuse and Mental Health Services Administration

What We Learned (1)

- In the paper world, providers and staff attempted to honor patient requests not to disclose sensitive information by redacting it by hand (or potentially omitting it from records where possible).
  - Less than perfect – inferences from other data and "leakage" were still possible (e.g., data in notes).
- Some HIEs will not accept information from Part 2 providers/programs, but some private HIEs have been established (for ex., Arizona).

What We Learned (2)

- Behavioral health provider obtains required authorization from patient to disclose information to another care provider.
- DS4P technology tags a CCDA (or individually disclosed data element) coming from the behavioral health provider, in the payload and/or metadata, with an indication that the document is restricted and cannot be redisclosed without further authorization from the patient.

What We Learned (3)

- A recipient provider using DS4P would have the capability to **view** the restricted CCDA (or data element) but the CCDA or data cannot be automatically parsed/consumed/inter-digitated into the EHR
  - Doing so would risk possibly re-disclosing sensitive data without patient authorization.
- Recipient providers not using DS4P could not view the information.

What We Learned (4)

- Implementation to date has largely been "all in" or "all out" with respect to disclosure of information from behavioral health providers/programs
  - The restriction tag in the CCDA applies to the entire document.
  - Granularity with respect to information shared by a behavioral health provider might be achieved by omitting information from the CCDA. (But that raises the "Swiss cheese" problem, and providers don't know data are missing.)

What We Learned (5)

- Next steps for technology companies working on this:
  - enabling query of behavioral health providers (transmittal of authorization);
  - enabling decision support without risking unauthorized re-disclosure; and
  - parsing.

Straw Recommendations Discussion (1)

- DS4P is not a perfect solution – but could be the on ramp/first step to enable sharing of information by behavioral health providers with other providers caring for behavioral health patients.
- "View only" is less than ideal – but many providers may feel that having access to some data about their patients is better than having none.
- All or nothing is also less than ideal – but provides a way for information to be disclosed from behavioral health providers when patients provide authorization (which occurs 90+ percent of the time)

Straw recommendations discussion (2)

- Certification of both behavioral health EHRs and provider EHRs for the DS4P technical capability will enable the sharing of data protected by Part 2.
  - Should this be mandatory for CEHRT?
- Functionality will be present – but providers still reluctant to accept data that cannot be populated into the EHR should not be required to use it.
  - E.g., no MU requirement – but potential for future menu option for EPs and EHs, or make receipt of data from BH providers eligible to "count" for meeting information exchange requirements?

Straw recommendations discussion (3)

- Education of providers and patients is, once again, key
  - What are the limits of the technology?
  - Additional clarifying guidance (esp. for non-behavioral health providers/programs) re: Part 2 obligations (particularly when information is provided “by the patient”)?

Results of Discussion to Date

- The Tiger Team had a robust discussion about these potential recommendations.
  - Some of the key questions raised are included in the back up slides.
- While some members thought that this functionality had been sufficiently piloted and ought to be in EHRs (leaving to the HITSC the question of whether the specific standard is mature enough for certification requirements); others thought that the workflow issues had not been worked through sufficiently and thus, should remain in the pilot phase.

Results of Discussion to Date

- As a result, the Tiger Team agreed to continue the discussion in May with a goal of presenting final proposed recommendations to the HITPC in June.
- The Tiger Team invites preliminary views from the HITPC on the straw recommendations and discussion thus far to inform its deliberations going forward.

Privacy and Security Tiger Team

BACK UP SLIDES

Workflow Issues

- How to best indicate/organize sequestered documents.
- Functionality that allows providers to summarize sequestered documents and make notes re: treatment decisions made based on information contained in sequestered documents.
- Preventing providers from overusing DS4P (i.e. tagging documents as “sensitive” that are not, which would lead to documents not getting integrated into the recipient EHR).
- Functionality that allows potential recipients to block receipt of sensitive documents/notifies senders when this action is taken.

Other Questions (1)

- Additional guidance needed from SAMHSA?
  - How should recipients handle data that comes in from BH providers with restricted tags?
  - Are there ways providers can work with patients to get them comfortable with having their information interdigitated into the EHR?
- Can a BH provider receive consent for ongoing release, or does consent need to be provided on a release by release basis?
- Can a provider refuse to treat patients unless they agree to have their behavioral health information added to the EHR?

Other Questions (2)

- Straw approach would allow for greater piloting, but at the same time invites vendors to integrate functionality.
  - It is unclear to what extent more DS4P pilots are needed and whether additional piloting should preclude certification/vendors' ability to integrate functionality
- Is there a better approach out there?
- Is having such functionality desirable? (Note: The maturity of the standards used to accomplish this functionality is a standards committee question).