Health IT Policy Committee

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

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

June 10, 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
- **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.
- **Kitt Winter,** Member, Social Security Administration
- **Stephania Griffin,** Ex Officio, Veterans Health Administration
- **Linda Sanches,** Ex Officio, HHS – Office for Civil Rights
- **Andrea Wilson,** Ex Officio, Veterans Health Administration

Background on 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, 2014 meeting

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.

HITPC Transmittal Letter, September 1, 2010. http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf

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 use of EHRs may create expectation of more complete information

State of Technology – DS4P

- DS4P = 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).
- 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 how Part 2 data is handled today by providers and some HIEs.

Glide path for Senders of Part 2-Protected Data (Part 2 Providers)

Level	Status	Description
0	Current State	Sender cannot send patient information electronically without some technical capability to indicate information is subject to restrictions on re-disclosure consistent with Part 2. Sender also has to have confidence that receiver can properly handle electronically sent Part 2-covered data.
1	Document-Level Sequester	With authorization from the patient, sender EHR can send CCDA tagged as restricted and subject to Part 2 restrictions on re-disclosure.

Glide path for Recipients of Part 2-Protected Data

Level	Status	Description
0	Current State	Part 2-covered data is not provided electronically to general healthcare providers. The status quo remains to share Part 2-covered data via paper, fax, etc.
1	Document-Level Sequester	Recipient EHR can receive and automatically recognize documents from Part 2 providers, but the document is sequestered from other EHR data. 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. Document level tagging can help prevent re-disclosure.
2	Local Use Only Solution	Recipient EHR can parse and extract data from structured documents from Part 2 providers for use in local CDS and quality reporting engines, but data elements must be tagged and/or restricted to help prevent re-disclosure to other legal entities through manual or automated reporting or interfaces. This would allow the data to be used locally for CDS but would not require complicated re-disclosure logic for the EHR vendor (i.e. Processes around re-disclosure are not well-defined).
3	EHRs for General Use and Sharing Advanced Metadata and Re-disclosure*	Recipient EHR can consume patient authorization for re-disclosure from Part 2 provider and act on such authorizations at a data-level. At a minimum, the recipient EHR would need to make the user aware of whether additional Part 2 consent is required before re-disclosing any particular data element to another legal entity, and allow recording of patient authorization for re-disclosure at the data-level. Processes for re-disclosure are well-defined.

*General Use EHR that makes optimal use of Part 2 data

Recommendations - Technical Capabilities

- Ideally for MU 3, include level 1 send and receive functionality in voluntary certification program for BH providers
  - BH EHRs must be able to control which recipients can be sent Part 2-covered electronic documents
- Ideally for MU 3, include level 1 receiver functionality as voluntary certification criterion for CEHRT*
  - Only recipient providers interested in being at level 1 would request capability from vendors.
  - Moving from sender status quo – 0 – requires level 1 capabilities for sender and at least level 1 capabilities for recipient.
- Level 2 and 3 are beyond MU 3
  - However, progression less likely to occur if we don't lay the foundation for moving from level 0 to level 1 for both BH and EP/EH EHRs

*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

Note: Providers may desire to implement greater role-based access controls for Part 2 Data

Recommendations – Policy & Best Practices

- Additional pilots and guidance needed to clarify recipient response.
  - Sending providers should send restricted CCDAs only to recipients interested and able to receive them electronically; should this be done contractually? Informally? Can technical mechanisms be developed to indicate recipient status?
  - Identify unanticipated workflows and consequences resulting from physicians and staff using EHRs with level 1 functionality
  - Determine how recipient EHRs will be able to re-release Part 2 data if patient gives authorization
  - Additional pilots will enable understanding of what the rules for accepting the obligations under levels 2 and 3 might be.
- Education of providers and patients is, once again, key.
  - Obligations that come with Part 2 data, especially around re-disclosure, are not yet fully understood.
  - SAMHSA should provide additional written guidance on how to operationalize statutory requirements in a digital environment:
    - Specifically on how recipients are expected to handle a restricted CCDA.
    - Clarifying the circumstances under which this information can be subsequently "sourced" from the patient in an informed way
    - SAMHSA should gather user feedback to ensure that new guidance does not impose workflow barriers that would substantially inhibit existing or future flow of information Part 2 information

Recommendations (3)

- The HITSC should address the following:
  - Is DS4P or any other standard mature/feasible enough for BH EHR voluntary certification, and if so, at what level of granularity?
  - Is DS4P or any other standard mature/feasible enough for general EHR voluntary certification, and if so, at what level of granularity?

Privacy and Security Tiger Team

BACK UP SLIDES

Background on Federal Confidentiality Law

(a) Requirement

Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall, except as provided in subsection (e) of this section, be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under subsection (b) of this section.

(b) Permitted disclosure

(1) Consent

The content of any record referred to in subsection (a) of this section may be disclosed in accordance with the prior written consent of the patient with respect to whom such record is maintained, but only to such extent, under such circumstances, and for such purposes as may be allowed under regulations prescribed pursuant to subsection (g) of this section.

42 U.S.C. § 290dd-2: Confidentiality of Records, http://www.gpo.gov/fdsys/pkg/USCODE-2011-title42/pdf/USCODE-2011-title42-chap6A-subchapIII-A-partD-sec290dd-2.pdf

Background on Federal Confidentiality Law (2)

(b) Permitted disclosure (cont'd)

(2) Method for disclosure

Whether or not the patient, with respect to whom any given record referred to in subsection (a) of this section is maintained, gives written consent, the content of such record may be disclosed as follows:

(A) To medical personnel to the extent necessary to meet a bona fide medical emergency.

(B) To qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation, but such personnel may not identify, directly or indirectly, any individual patient in any report of such research, audit, or evaluation, or otherwise disclose patient identities in any manner.

(C) If authorized by an appropriate order of a court of competent jurisdiction granted after application showing good cause therefor, including the need to avert a substantial risk of death or serious bodily harm. In assessing good cause the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician- patient relationship, and to the treatment services. Upon the granting of such order, the court, in determining the extent to which any disclosure of all or any part of any record is necessary, shall impose appropriate safeguards against unauthorized disclosure.

42 U.S.C. § 290dd-2: Confidentiality of Records, http://www.gpo.gov/fdsys/pkg/USCODE-2011-title42/pdf/USCODE-2011-title42-chap6A-subchapIII-A-partD-sec290dd-2.pdf

Clarifying Guidance on Part 2

- **Under Part 2, can an HIO or HIO affiliated member use a consent form that generally designates the entities permitted to make disclosures of Part 2 information, and refers to the HIO's website for a list of those disclosing entities?**
  - Yes, the consent form can refer to the HIO's website for the list of entities permitted to make disclosures if the *disclosing entity* is identified by a "general designation" in the consent form as permitted under Part 2. Part 2's consent provisions allow either the "name or general designation of the program or person permitted to make the disclosure" to be specified on the consent form. Because a general designation is permitted, if such general designation is used, then the specific names of those disclosing entities do not need to be included on the consent form and patients can be referred to the HIO's website for a list of those entities.
  - This is in contrast to Part 2's consent provision regarding *recipients* of Part 2 data. 42 CFR §2.31(a)(2) requires that a consent form include "the name or title of the individual or the name of the organization to which disclosure is to be made." Thus, as was previously noted in previously issued FAQ Number 18 published by SAMHSA and ONC in 2010 (www.samhsa.gov/healthPrivacy/docs/EHR-FAQs.pdf (PDF | 381 KB)), Part 2 consents cannot refer patients to the HIO's website for a list of potential recipients of their data but rather must identify within the consent all the HIO affiliated members by name or title that are potential recipients of the Part 2 data. Therefore, a new consent form (e.g. by the additional Part 2 program or the HIO) would be required when a new recipient of the information is added.

"Substance Abuse and Mental Health Services Administration (SAMHSA) Guidance - *Applying the Substance Abuse Confidentiality Regulations, 24 CFR Pt. 2 FAQs*: http://beta.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs.

Clarifying Guidance on Part 2 (2)

- **Under what circumstances can information disclosed pursuant to Part 2 be redisclosed?**
  - Once Part 2 information has been initially disclosed (with or without patient consent), no redisclosure is permitted without the patient's express consent to redisclose or unless otherwise permitted under Part 2.
  - Disclosures made *with* patient consent must be accompanied by a statement notifying the recipient that Part 2 redisclosure is prohibited, unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by Part 2 (42 CFR § 2.32).
  - When disclosures are made *without* patient consent under the following circumstances, limited redisclosures without obtaining the patient's consent: are permitted, such as medical emergencies [42 CFR § 2.51], child abuse reporting [42 CFR § 2.12(c)(6)], crimes on program premises or against program personnel [42 CFR § 2.12(c)(5)], and court ordered disclosures when procedures and criteria are met [42 CFR §§ 2.61-2.67].

"Substance Abuse and Mental Health Services Administration (SAMHSA) Guidance - *Applying the Substance Abuse Confidentiality Regulations, 24 CFR Pt. 2 FAQs*: http://beta.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs.

Clarifying Guidance on Part 2 (3)

- When disclosures are made under the following circumstances the recipient is prohibited from redisclosing the information without consent, except under the following restricted circumstances:
  - **Research**: Researchers who receive patient identifying information are prohibited from redisclosing the patient-identifying information to anyone except back to the program [42 CFR § 2.52(b)].
  - **Audits and Evaluations**: Part 2 permits disclosures to persons and organizations authorized to conduct audits and evaluation activities, but imposes limitations by requiring any person or organization conducting the audit or evaluation to agree in writing that it will redisclose patient identifying information only (1) back to the program, or (2) pursuant to a court order to investigate or prosecute the program (**not** a patient), or (3) to a government agency that is overseeing a Medicare or Medicaid audit or evaluation [42 CFR § 2.53(c)(d)].
  - **Qualified Service Organization Agreements (QSOAs)**: Part 2 requires the QSO to agree in writing that in receiving, storing, processing, or otherwise dealing with any information from the program about patients, it is fully bound by Part 2, it will resist, in judicial proceedings if necessary, any efforts to obtain access to information pertaining to patients except as permitted by Part 2, and will use appropriate safeguards to prevent the unauthorized use or disclosure of the protected information [42 CFR § 2.11]. In addition, QSOAs may allow disclosure in certain circumstances.
  - **Authorizing Court Orders**: When information is disclosed pursuant to an authorizing court order, Part 2 requires that steps be taken to protect patient confidentiality. In a civil case, Part 2 requires that the court order authorizing a disclosure include measures necessary to limit disclosure for the patient's protection, which could include sealing from public scrutiny the record of any proceeding for which disclosure of a patient's record has been ordered [42 CFR § 2.64(e)(3)]. In a criminal case, such order must limit disclosure to those law enforcement and prosecutorial officials who are responsible for or are conducting the investigation or prosecution, and must limit their use of the record to cases involving extremely serious crimes or suspected crimes. For additional information regarding the contents of court orders authorizing disclosure, see 42 CFR § 2.65(e).

"Substance Abuse and Mental Health Services Administration (SAMHSA) Guidance - *Applying the Substance Abuse Confidentiality Regulations, 24 CFR Pt. 2 FAQs*: http://beta.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs.

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.

HITPC Transmittal Letter, September 1, 2010. http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf
Consumer Choice Technology Hearing, June 29, 2010. http://www.healthit.gov/sites/default/files/archive/index.php?dir=FACA%20Hearings/2010-06-29%20Policy%3A%20Privacy%20%26%20Security%20Tiger%20Team%2C%20Consumer%20Choice%20Technology%20Hearing

C&A Workgroup: Blog Comments on Voluntary EHR Certification for Behavioral Health and Long-Term and Post-Acute Care Settings

- The majority of public comments to date have related to privacy and security standards:
  - Any standards for the BH component needs to distinguish between Psychologists acting as a team member in the institutional setting, and those covering private ambulatory patients.
  - The standards need to be very explicit in how barriers are created, and what information is/is not 'protected'. How to incorporate this into a CCDA is even more challenging.
  - It would be useful for the proposed behavioral health certified EHRs to receive Meaningful Use information from other EHRs so that behavioral health providers could meet Meaningful Use standards.
  - It is very important for behavioral health-care providers to be able to mark every individual document as requiring specific consent or not.

Wolf, Larry. HealthIT Buzz. Seeking Your Feedback: Voluntary EHR Certification for Behavioral Health and Long-Term and Post-Acute Care Settings, May 14, 2014. http://www.healthit.gov/buzz-blog/federal-advisory-committees/seeking-feedback-voluntary-ehr-certification-behavioral-health-longterm-postacute-care-settings/