



Health IT Policy Committee

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

July 15, 2014

Karen DeSalvo, MD

National Coordinator for Health Information Technology

Department of Health and Human Services

200 Independence Avenue, S.W.

Washington, DC 20201

Dear Dr. DeSalvo:

The HIT Policy Committee (Committee) gave the following broad charge to the Privacy & Security Tiger Team (Tiger Team):

Broad Charge for the Privacy & Security Tiger Team

The Tiger Team is charged with making short-term and long-term recommendations to the Health Information Technology Policy Committee (HITPC) on privacy and security policies and practices that will help build public trust in health information technology and electronic health information exchange (HIE), and enable their appropriate use to improve healthcare quality and efficiency, particularly as related to American Recovery and Reinvestment Act (ARRA) and the Affordable Care Act (ACA) which mandates a number of duties to the Office of the National Coordinator (ONC) relative to privacy and security.

The Privacy and Security Tiger Team considered certification to enable exchange of behavioral health data in response to a request from the Certification & Adoption (C&A) Workgroup. The C&A Workgroup had proposed areas for privacy and security certification for all providers (MU and non-MU – specifically, behavioral health providers). In support of this effort, the Tiger Team invited data segmentation for privacy (DS4P) pilot participants, representatives from the Substance Abuse and Mental Health Services Administration, and other experts to share their experiences with DS4P and behavioral health data.¹ This letter provides the resulting recommendations, which were adopted by the Committee on June 10, 2014, to the National Coordinator, Department of Health and Human Services (HHS).

Background

In September 2010, the HITPC adopted recommendations regarding data segmentation following Tiger Team discussions and a hearing on Consumer Choice Technology.² The transmittal letter incorporated lessons learned from the initial hearing on data segmentation technologies and noted that technology to support more granular consent is “promising” but still in early stages of development and adoption. The letter suggested that granular consent should be a priority for ONC to explore further, through pilots. In the interim, the Tiger Team noted the importance of educating providers and patients

¹ Pilot participants, SAMHSA representatives, and experts presented their experiences at Tiger Team meetings on April 16, 2014, April 28, 2014, May 12, 2014, and May 27, 2014; some provided additional written responses to follow-up questions from the Tiger Team. <http://www.healthit.gov/facas/calendar/2014/4>

² Office of the National Coordinator, Consumer Choice Technology Hearing, June 29, 2010. <http://bit.ly/1ophnWQ>

regarding implications of consent decisions and potential limitations of technology approaches to consent management.³

The need to provide coordinated care for individuals with mental health and/or behavioral health issues was clear. Enhanced consent requirements for behavioral health data, 42 CFR Part 2, in particular, were implemented to address reluctance of individuals to seek care for behavioral health conditions.⁴ However, the ability of patients to withhold consent to disclose information remains a concern for providers. Providers want to provide the best care for patients, but they have concerns about incomplete records out of both professional obligation and liability considerations. While the need for providers to act on incomplete information is not necessarily new, the use of electronic health records (EHR) may create an expectation of more complete information.

DS4P was an initiative of ONC's Standards & Interoperability 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, the Tiger Team sought to understand more about the pilots completed to date, implementation instances of DS4P, and how Part 2 data is handled by providers and some HIEs today.

Framework for the Exchange of Behavioral Health Information

In recognition of the business, clinical, and technical complexities of this topic, the Tiger Team suggests a framework of two glide paths for the exchange of Part 2-protected data, based on whether the subject is sending or receiving information. The following two tables present the proposed glide path for moving forward.

Glide Path for Senders of Part 2-Protected Data

The first component of the framework is a glide path for senders of Part 2-protected data.

Table 1 Glide Path for Senders of Part 2-Protected Data

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-protected data.
1	Document-Level Sequester	With authorization from the patient, sender EHR can send Consolidated Clinical Document Architecture (CCDA) tagged as restricted and subject to Part 2 restrictions on re-disclosure.

³ HITPC Transmittal Letter, September 1, 2010. <http://bit.ly/1mUP9E1>

⁴ 42 CFR Part 2 pertains to federal regulations governing certain personal information collected by federally supported substance abuse treatment programs. <http://1.usa.gov/1kfdXlf>

Glide Path for Recipients of Part 2-Protected Data

A second component of the framework is a glide path for recipients of Part 2-protected data.

Table 2 Glide Path for Recipients of Part 2-Protected Data

Level	Status	Description
0	Current State	Part 2-protected data is not provided electronically to general healthcare providers. The status quo remains to share Part 2-protected 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 Clinical Decision Support (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.

Recommendations for Technical Capabilities

Ideally for meaningful use 3, the Tiger Team recommends including level 1 send and receive functionality in the voluntary certification program for behavioral health providers. This is a required criterion that is part of a voluntary certification program. Behavioral health EHRs must be able to control which recipients can be sent Part 2 –protected electronic documents. The Tiger Team also recommends including level 1 receiver functionality as a voluntary certification criterion for CEHRT. Only recipient providers interested in being at level 1 would request the appropriate capability from vendors.

Furthermore, moving from sender status quo at level 0 requires level 1 capability for the sender and at least level 1 capability for the recipient.

The Tiger Team is not suggesting that there be a meaningful use requirement. However, there is potential for future menu option for EPs and EHs, or to make receipt of data from behavioral providers eligible to “count” for meeting information exchange requirements related to transitions of care. At any level, providers may desire to implement greater role-based access controls for Part 2-protected data.

The Tiger Team acknowledges that levels 2 and 3 are beyond the applicable timeframe for meaningful use stage 3. However, the Tiger Team felt strongly that progression is less likely to occur if the HITPC does not lay the foundation for moving from level 0 to level 1 for both behavioral health providers and general EHRs.

Recommendations for Policy & Best Practice

The Tiger Team urges the development of additional pilots and guidance in order to clarify sender activities and the recipient response to Part 2-protected data. Pilots should do the following to promote greater understanding of the recipient response:

- Identify unanticipated workflows and consequences resulting from physicians and staff using EHRs with level 1 functionality;
- Enable understanding of what the rules for accepting the obligations under levels 2 and 3 of the glide path might be; and
- Address how recipient EHRs will be able to re-release Part 2-protected data if a patient gives authorization.

In addition, the Tiger Team recommends that the pilots address the following sender-related questions:

- Sending providers should send restricted CCDAs only to recipients interested and able to receive them electronically. Can this be done contractually or informally?
- Can technical mechanisms be developed to indicate recipient status (e.g. Level 0: Current State, Level 1: Document-Level Sequester)?

The education of providers and patients remains key. Obligations that come with Part 2-protected data, especially around re-disclosure, are still not fully understood. In particular, the Tiger Team recommends that SAMHSA provide additional written guidance on how to operationalize statutory requirements in a digital environment through:

- Specific instruction on how recipients are expected to handle a restricted CCDA; and
- Clarification on the circumstances under which information can be subsequently “sourced” from the patient in an informed way as opposed to coming from the Part 2 provider.

The Tiger Team also recognizes the value of user feedback through the guidance process. Any new guidance should not impose workflow barriers that would substantially inhibit existing or future flow of information Part 2-protected data.

The Tiger Team recommends that the Health Information Technology Standards Committee 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?

As noted previously, the Policy Committee adopted these recommendations at its June 10, 2014 meeting. We appreciate the opportunity to provide these recommendations and look forward to discussing next steps.

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee