Health IT Policy Committee

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

Privacy and Security Tiger Team

Today's Discussion:

Virtual Hearing Update and Data Intermediaries

November 6, 2013

Tiger Team Members

- **Deven McGraw, Chair,** Center for Democracy & Technology
- **Paul Egerman, Co-Chair,** Entrepreneur
- **Dixie Baker,** Martin, Blanck, and Associates
- **Judy Faulkner,** Epic Systems Corporation
- **Leslie Francis,** University of Utah College of Law
- **Gayle Harrell,** Consumer Representative/Florida
- **John Houston,** University of Pittsburgh Medical Center
- **David McCallie,** Cerner Corporation
- **Wes Rishel,** Gartner
- **Micky Tripathi,** Massachusetts eHealth Collaborative
- **Kitt Winter,** Social Security Administration

Agenda

- Quick status on Virtual Hearing for Accounting of Disclosures*
  - Held on September 30, 2013
  - Currently deliberating on results and expect to present at the December HITPC meeting
- Results of Deliberations on Privacy and Security Considerations for Data Intermediaries

*Additional information in attached backup slides

Background: Data Intermediaries

- In advance of Stage 3 of the EHR Incentive Program, the HIT Policy Committee (HITPC) and the Quality Measures Work Group (QMWG) convened a subgroup, the Data Intermediary Tiger Team (DITT) to make recommendations on data intermediary roles, including those related to privacy and security.
- Aim is to have a certification criteria that will allow data intermediaries to serve as the module for quality reporting functionality.

Data Intermediaries: Goals

- HITPC Privacy and Security Tiger Team asked to provide guidance on whether there are privacy and security considerations to be addressed as part of the certification process for data intermediaries.

P&S TT Recommendations on Third Party Intermediaries, September 2010

- **Collection, Use and Disclosure Limitation**: Third party service organizations may not collect, use or disclose personally identifiable health information for any purpose other than to provide the services specified in the business associate or service agreement with the data provider, and necessary administrative functions, or as required by law.

- **Time limitation**: Third party service organizations may retain personally identifiable health information only for as long as reasonably necessary to perform the functions specified in the business associate or service agreement with the data provider, and necessary administrative functions. Retention policies for personally identifiable health information must be established, clearly disclosed to customers, and overseen. Such data must be securely returned or destroyed at the end of the specified retention period, according to established NIST standards and conditions set forth in the business associate or service agreement.

- **Openness and transparency**: Third party service organizations should be obligated to disclose in their business associate or service agreements with their customers how they use and disclose information, including without limitation their use and disclosure of de-identified data, their retention policies and procedures, and their data security practices.

P&S TT Recommendations on Third Party Intermediaries, September 2010 (continued)

- **Accountability**: When such third party service organizations have access to personally identifiable health information, they must execute and be bound by business associate agreements under the Health Insurance Portability and Accountability Act regulations (HIPAA). However, it's not clear that those agreements have historically been sufficiently effective in limiting a third party's use or disclosure of identifiable information, or in providing the required transparency.

- While significant strides have been made to clarify how business associates may access, use and disclose information received from a covered entity, business associate agreements, by themselves, do not address the full complement of governance issues, including oversight, accountability, and enforcement. We recommend that the HIT Policy Committee oversee further work on these governance issues.

6

Discussion: Key Points

- Past recommendations on data intermediaries are sound but did raise concern about adequacy of BAAs in limiting BA disclosure and use and in promoting transparency.
- Tiger Team deliberated on potential vehicles for implementing its previous recommendations on data intermediaries:
  - MU3 requirements and/or
  - CMS Proposed Rule on Revisions to Payment Policies under Physician Fee Schedule (78 FR 43362; 7/19/2013)*

*See: http://www.gpo.gov/fdsys/pkg/FR-2013-07-19/pdf/2013-16547.pdf

- CMS NPRM proposes quality clinical data registries or QCDRs* **must enter into and maintain with its eligible professionals appropriate BA agreements** that provide for QCDRs receipt of patient specific data from the EPs as well as the QCDRs public disclosure of quality measure results.

*The NPRM proposed to define a ‘‘qualified clinical data registry’’ (QCDR) for purposes of the PQRS as a CMS-approved entity (such as a registry, certification board, collaborative, etc.) that collects medical and/or clinical data for the purpose of patient and disease tracking to foster improvement in the quality of care furnished to patients.

Options Discussed

- Under one or both of these rules, require providers to:
  - Attest that any business associate agreement (BAA) with a data intermediary provides for transparency to the provider* of data uses and disclosures of health information by the BA and
  - Provide a copy of BAA provisions focused on transparency
- Another option may be to define quality measures that only use data already in the EHR, thus limiting the number of intermediaries involved.

*Providers have the option of disclosing these data uses to patients in their HIPAA Notice of Privacy Practices or other transparency venues.

Conclusions

- Ultimately, the TT concluded there was not an appropriate policy vehicle to hold BAs accountable for greater transparency to providers around their uses and disclosures of identifiable health information.
- Regarding a possible attestation requirement, the Tiger Team:
  - concluded that attempting to hold providers accountable for the behavior of data intermediaries was problematic and there was a lack of policy vehicles available to directly regulate these entities.
  - noted the potential large number of data intermediary BAs and difficulties in identifying them and defining exactly what is meant by "BAA provisions regarding transparency."
  - reserves the option, as always to revisit this issue as the environment continues to evolve.

Key Discussion Points

- Nonetheless, the Tiger Team would like to share key points raised during its deliberations and offer these to the HITPC for further discussion and consideration.
- The discussion highlighted a serious concern that the superior bargaining power of large data intermediary BAs results in providers being "forced" to agree to BAAs/DUAs granting BAs broad rights to future uses and disclosures of provider data.

Key Discussion Points

- Specifically, the Tiger Team saw the following as issues:
  - Patient control & autonomy – patients have no say in whether or how data intermediaries use their information; further, these uses are not transparent to patients
  - Proliferation of data intermediaries – the larger the number of data intermediaries that hold patient data, the greater the risk that problems will occur

Key Discussion Points

- This discussion led the Tiger Team to the belief that from a privacy and security standpoint, it may be desirable to define quality measures in such a way that they can be derived from the data already in EHR systems, thus limiting the number of of data intermediaries that need to be involved.
- The Tiger Team
  - recognized that other balancing factors may need to be considered and
  - concluded that such a recommendation would be beyond its scope, but offers it to the HITPC for further consideration.

Data Intermediaries

BACKUP SLIDES

Hearing: Accounting of Disclosures

- Held at request of OCR on Monday, September 30, 2013
- Testimony from providers, patient rights organizations, vendors and business associates, and health plans.
- Received written comments from the public through ONC's blog as well as public comments at the hearing.
- Currently, analyzing the results and plan to report recommendations at the Nov HITPC

Panelists

Panel I: Patient Perspectives

- Mark Richert, Esq. - Director, Public Policy; *American Federation for the Blind*
- Joanne McNabb – Director of Privacy Education and Policy; *California State and Consumer Services Agency*
- Dr. Deborah Peel – Founder; *Patient Privacy Rights*
- Michelle de Mooy – Senior Associate, National Priorities; *Consumer Action*

Panel 2: Vendor/Business Associate Perspectives

- Kurt Long – Chief Executive Officer and Founder; *FairWarning*
- Eric Cooper - Health Information & Identity Management Product Lead; *EPIC*
- Jeremy Delinsky - Chief Technology Officer; *Athena Health*
- John Travis - Senior Director, Regulatory Compliance; *Cerner* accompanied by Lori Cross – Director of Laboratory Operations; *Cerner*

Panelists

Panel 3: Provider Perspectives

- Darren Lacey – Chief Information Security Officer; *Johns Hopkins University Health System*
- Lynne Thomas Gordon – Chief Executive Officer; *American Health Information Management Association*
- Jutta Williams – Director, Corporate Compliance Privacy Office; *Intermountain Healthcare*
- William Henderson – Administrator, *The Neurology Group, LLP (Albany, NY)* and Co-Chair, *Board of Directors of Medical Group Management Association*
- Kevin Nicholson – Vice President, Public Policy and Regulatory Affairs; *National Association of Chain Drug Stores*

Panel 4: Payer Perspectives

- Scott Morgan – Executive Director, National Privacy and Security Compliance Officer; *Kaiser Permanente*
- Jay Schwitzgebel – Director Information Security & IT Compliance; *Caresource*

DATA INTERMEDIARIES: CONTEXT

① Provider inputs information into EHR.
② EHR performs the **capture**.
③ DI **calculates** data analytics on behalf of provider and **reports** clinical quality data to CMS/Payer.
④ CMS/Payer transmits back to provider or to DI (which sends to provider) for quality improvement.

TOGETHER = module performing requisite functionality