Update from the Health IT Policy Committee's Privacy & Security "Tiger Team"

Deven McGraw
Partner
Manatt, Phelps & Phillips LLP
September 24, 2014

What is the Tiger Team?

- Health IT Policy Committee = created by HITECH to advise ONC on policy issues arising out of implementation of the EHR incentive program and related provisions.
- The Privacy and Security "Tiger Team" – part of HIT PC; initially formed in summer 2010 to quickly come up with recommendations on consent for electronic health information exchange.
- The name stuck – until now. The Privacy & Security working group will begin anew in October.

Workgroup charge

- 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.

Busy past year

- Data segmentation (June 2014)
- Accounting of Disclosure (December 2014)
- Improving “meaningful use” security risk assessment compliance (October 2013)
- Access to “view/download/transmit” by proxies (April 2014)
- Queries for patient records (February 2013)

Data Segmentation (aka DS4P)

- Issue: Can EHRs help providers implement granular consent laws?
- First took this issue on back in 2010-2011: some uptake of data segmentation technologies but not widespread. Pilots needed.
- Post DS4P pilots: ready for certification requirements?
- Considered in the context of behavioral health data subject to 42 CFR Part 2.

Challenges

- Providers covered by Part 2 cannot disclose information without the authorization of the patient and need to “flag” that the information cannot be further redisclosed without authorization.
- Pilots had successfully tested technologies that enabled a document to be sent “read only” (to prevent inadvertent re-disclosure).
- So disclosure could occur – but information could not be integrated into the recipient EHR.

Recommendations

- For behavioral health providers, certification must include DS4P capability.
- For non behavioral health providers, optional to include this capability. (vendors)
- Although technical capabilities still limited, felt it was important to take this first step.
- Urged SAMHSA to provide more guidance and even re-examine rules appropriate to digital environment.

Accounting of Disclosures

- HIPAA regulations provide patient with right to request accounting of disclosures of PHI – but disclosures for TPO excluded.
- HITECH: if disclosures are through an EHR, no exclusion for TPO.
- HHS required to come up with regulations that takes into account both individuals' interests in learning about disclosures from their records and burden on covered entities.

History

- Proposed regulation to implement this change created two rights for patients:
  - Accounting of specific disclosures (not TPO)
  - Access report of individuals who have accessed a patient's record.
- EHR certification requirements included voluntary certification criterion to try to implement; no known uptake.

Virtual hearing

- Transparency to patients about what happens to their health information is important.
- However, no testimony supported that the proposed access report was do-able, at least with current technologies.
  - Also unlikely to be of much use to patients.
- Automated capture of external disclosures more feasible.

Recommendations

- Implement in a step-wise fashion, focusing first on provider EHRs.
- Focus on:
  - patient's right to a report of "external" disclosures (outside of the entity or OHCA).
  - Patient's right to an investigation of potential inappropriate internal access.
- Pilot technologies first – then implement what is achievable by the technology.

Recommendations (cont.)

- To improve ability for covered entities to detect inappropriate internal access, OCR should add two implementation specifications to the current audit control standard in the HIPAA Security Rule (164.312(b)):
  - (Addressable) Audit controls must record PHI-access activities to the granularity of the user (workforce member or natural person) and the individual whose PHI is accessed.
  - (Addressable) Information recorded by the audit controls must be sufficient to support the information system activity review required by §164.308(a)(1)(ii)(D) and the investigation of potentially inappropriate accesses of PHI.
- Note: we did not recommend that these reports of individual access to reportable to the individual.

Improve MU Security Risk Assessment

- For Stage 3 of MU, we did not seek additional MU objectives regarding security – but sought instead to improve accountability with the existing requirement to perform a security risk analysis and correct identified deficiencies.

Recommendations

- Emphasize that attestation to completion of the MU security risk assessment = attesting to compliance with the HIPAA Security Rule re: that analysis.
- Require entities to identify the individual(s) responsible for conducting and documenting the risk assessment.

Recommendations (cont.)

- Link attestation to specific MU objectives, rather than as a single stand-alone measure. Specifically, require that a risk analysis has been performed on any new functionality provided due to deployment of new objectives or CEHRT criteria.
- CMS and OCR should also provide more education on expectations and importance of conducting and documenting the security risk analysis and correcting deficiencies.

Proxy Access to V/D/T

- Stage 2 of Meaningful Use requires 50% of patients be provided with the capability to view, download and transmit relevant information from the EHR.
- Question arose about access by friends, family and personal representatives.
- No new policy needed – but lots of uncertainty about how to implement. Urged ONC to develop & disseminate best practices for assuring access to adult patient V/D/T can be extended to friends & family authorized by the patient and, where appropriate, to legal personal representatives.

Recommendations

- Covered authorization to access
  - For friends & family, easiest case is when patient makes request; otherwise, must confirm with patient.
  - LPR status depends on state law; providers need to adapt process they use for paper records for electronic.
- Identity proofing & authentication – rely on prior Tiger Team recommendations on id proofing and authenticating patients for V/D/T.

Recommendations (cont.)

- Education of patients about scope of V/D/T access, and functionalities, so they can make informed choices w/r/t friends and family.
- For LPR access, need to make sure that access granted by law is consistent with the type of access granted through V/D/T.

(if time) Queries

- Another area where law was sufficient but guidance to providers was needed.
- Considered three scenarios/use cases:
  - Query to one or more specific providers (targeted), HIPAA controls.
  - Query to one or more specific providers, data covered by more stringent consent law
  - Query based on patient demographics, using aggregator to find patient (non-targeted)

Existing Obligations

- Data holder (response)
  - Needs reasonable assurance as to entity requesting data
  - Needs reasonable assurance that querying entity has, or is establishing, a direct treatment relationship with the patient
  - Makes decision about whether to release data, and if so, what data, consistent with law.
  - If responding, needs to send back data for right patient, needs to properly address request, needs to send securely. (may need to communicate need for consent and confirm it exists/place in file where required)
- [Not on list: needs to be certain of privacy protections adopted by recipient!]

Existing Obligations

- Requester (query)
  - Needs to present identity credentials
  - Must demonstrate (in some way) the treatment relationship
  - Must send patient identifying information in a secure manner to enable data holder to locate the record.
  - (may need to send consent in circumstances where it is required)

Recommendations

- Essentially list of best practices for meeting each of the obligations. For example:
  - Data holders may be reasonably assured of a requester's identity through, for example, the use of DIRECT certificates, membership in a trusted network, or a pre-existing relationship. (other examples)
  - Data holders may be reasonably assured of a treatment relationship if, for example, there is prior knowledge of the relationship, the relationship can be confirmed within a network, or if the requester provides some communication of consent. (other examples)

Recommendations

- Queries should be logged, and the log should be available to patients upon request. (Note that we completed recommendations on query before taking up accounting of disclosures.)
- Patients should have "meaningful choice" about whether they are listed in an aggregator service for nontargeted queries. (Came from our 2010 recommendations on consent.)

What's next?

- Privacy and Security workgroup – with a new co-chair (Stan Crosley) and some new members – begins again in October.
- First up: review of ONC's draft interoperability roadmap (focusing, of course, on privacy and security issues).

Thank you!

- Deven McGraw

  Partner

  Manatt, Phelps & Phillips, LLP

  dmcgraw@manatt.com

  202-585-6552