patientprivacyrights

Sept 30, 2013

Deven McGraw, Chair
Paul Egerman, Co-Chair
HIT Policy Committee's Privacy and Security Tiger Team
Office of the National Coordinator for Health IT

Re: Virtual Hearing on Accounting for Disclosures

Dear Deven and Paul:

Patient Privacy Rights (PPR) is the leading national consumer voice for building ethical, trustworthy HIT systems. We have 12,000 members in all 50 states and also represent 10.3 million Americans through our leadership of the bipartisan Coalition for Patient Privacy (see: http://patientprivacyrights.org/coalition-patient-privacy/). The Coalition:

- Seeks to restore the right of consent and the right to health information privacy in electronic health systems and data exchanges. Consent and control are imperative for patients to be willing to participate in and trust in electronic health systems and data exchanges.
- Expanded FIPPs for healthcare and developed the PPR Trust Framework, 75+ auditable criteria that enable the public to easily see which companies, websites, platforms, and applications meet their expectations for privacy in electronic systems.

The Accounting for Disclosures (AODs) provision was one of 6 new consumer protections we sought to include in HITECH. The bipartisan Coalition for Patient Privacy urged Congress to include historic new privacy and security rights in the Health Information Technology for Economic and Clinical Health (HITECH) Act.[1]

- The other 5 key protections are: a ban on sales of protected health information (PHI) without consent, the ability to segment sensitive PHI, meaningful breach notice, the right to block disclosure of protected health information PHI for healthcare operations (HCO) if treatment is paid for out-of-pocket, and encryption.

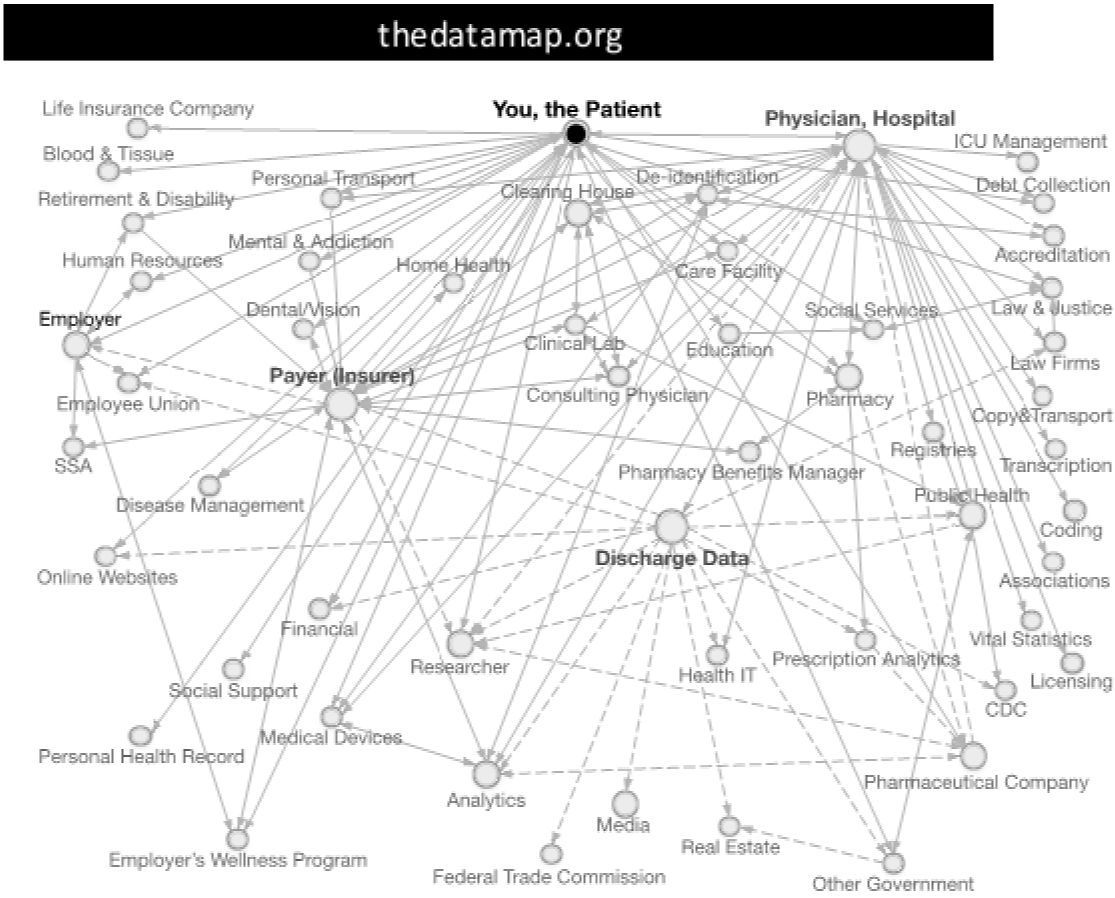
PPR was very involved in the regulatory process for AODs following HITECH.

- We submitted detailed letters about the NPRM and requirements for AODs in 2010 and 2011[2]. The 2011 letter has a section on the history of the AOD requirement.

[1] See the Coalition's letter to Congress on HITECH at: http://patientprivacyrights.org/wpcontent/uploads/2013/08/CoalitionPatPriv_Final01.14.091.pdf

[2] See Appendix for PPR's 2010 and 2011 letters to the Office of Civil Rights about the Accounting for Disclosures provisions in HITECH.

Current health IT systems: hidden data flows[3] and data analytics[4]



Patients can't get electronic copies of their health information, but a broad array of hidden users can, see thedatamap.org above. Few have direct relationships with patients.

"Today the healthcare analytics market has exploded." [5] Aetna/ActiveHealth Management, The Advisory Board Company, athenahealth, Caradigm, CareEvolution, Cerner, Explorys, Health Catalyst, Humedica/Optum, IBM, InterSystems, McKesson/MedVentive, Truven Health Analytics, and Wellcentive are all major players in this giant new market. All of them seek to acquire and use more and more patients' PHI. Two examples:

- "Optum and its founding partner, Mayo Clinic are making their information assets (109M lives of claims data, 35M lives of EHR data)." [6]
- Explorys' "customers span 14 major integrated healthcare systems with over 100 billion data elements, 40 million cared for lives, 200 hospitals, and over 100,000 providers." [7]

[3] thedatamap.org

[4] http://www.chilmarkresearch.com/chilmark_report/2013-clinical-anaytics-for-pop-health-market-trends-report/

[5] Ibid.

[6] http://strataconf.com/rx2013/public/schedule/detail/29813

Massive information asymmetry is a key reason that the billions spent on health IT failed to achieve the Triple Aim: lowering costs, improving health, and improving care. Health data is controlled by data holders that don't want to be transparent or accountable.

HIPAA states patients should have been able to automatically receive copies of PHI since 2001 and HITECH states patients should have been able to receive AODs since 2009. Surely it's time to ensure patients' federal rights to access PHI and AODs are finally honored.

Implementing robust AODs using Blue Button Plus and Direct will spur innovation, lower costs, improve health, and improve care

Most of the billions spent on health IT was wasted supporting the high-cost status quo. The systems and technologies implemented so far:

- Lock patients out of access to their own data.
- Violate patients' rights to privacy and control over PHI.
- Prevent transparency and accountability.
- Destroy the patient-physician relationship. Physicians can't act as patients' stewards to protect PHI from hidden use, disclosure, and sale.
- Support institutional control over PHI.
- Fail to lower costs, improve quality or improve care.

When patients can get their own data, innovators will finally build technology to serve them instead of large enterprises. Patients will be able to share PHI and use applications to:

- Independently audit their records for errors and breaches
- Receive independent decision support and advice
- Compare cost and quality of care
- Donate data for research they support

According to Harvard Prof. Clay Christensen, "Companies fail by listening to their customers, constantly improving products and services, and maximizing profits…They fail to do something counterintuitive: pursue new opportunities at the low end of their markets. [8]" The customers of HITECH Certified EHR Technology are not the patient and her physician who have become simply subjects of an increasingly hidden health-industrial complex.

Patients and patient advocates are the new opportunity at the low end of the healthcare market. Eager to use PHI, they are very motivated to seek high quality treatment and the best physicians, understand risks, support breakthrough research, lower treatment costs, prevent errors, and identify data breaches. The Tiger Team should empower patients and create new markets to serve them by giving them their daM data[9].

[7] https://www.explorys.com/about-us

[8] http://www.businessweek.com/articles/2012-05-03/clay-christensens-life-lessons

[9] http://www.youtube.com/watch?v=0gpk-fbfg4Y

Recommendations to quickly implement AODs using existing HIT and MU

The Tiger Team should:

- **Acknowledge that AODs implicitly require that patients can see which data are used or disclosed**, along with information from access logs that contain dates, times, names of those who used/disclosed the patient's data, the purpose of the use/disclosure, and who received it. AODs would obviously be meaningless if patients can't know what information was used or disclosed.

- **Automate the process of creating and transmitting AODs & PHI in the following ways**:
  - Data holders should create **patient and physician portals**
  - **Patient voluntary email address(es) should be used for data exchange** and RLS directories to enable segmentation
  - Patients and physicians should be able to **use the Direct Project to securely exchange data**
  - **Automate BB/ Blue Button Plus** so patients can view, download, and transmit PHI and AODs
  - **Enable patients to get PHI in 'real time'.** HIPAA allows for delays, but all AODs should be designed for automatic transmission in 'real time'. A physician should be able to override institutional policies that delay transmission of AODs or PHI.
  - **Automate AOD log entries to include**:
    - a copy of the data used or disclosed (or a link to the data)
    - the AOD log information: who used or sent the data and who received it
    - the purpose of the use or disclosure
  - **Automate** patients' ability to 'pull' AODs or automatically or 'push' AODs each time there is an AOD entry (or periodically) to:
    - a data base (such as a health data bank account)
    - an auditor or a designated agent

Summary: Instead of setting up new separate processes or acquiring new technologies to build, manage, and transmit AOD information and logs, the Tiger Team should recommend implementing AODs by 'piggybacking' on top of other key HIT initiatives already underway:

- CEs should use the Direct Project to securely transmit AODs and PHI to patients
- Automate Blue Button / Blue Button Plus
- Use existing data security technologies for authentication and auditing employees' access, use, and disclosure of PHI
- Automating AODs and obtaining copies of PHI is the cheapest, fastest, and simplest way to enable innovation and achieve the Triple Aim.

Conclusion

Congress very deliberately required AODs for TPO uses and disclosures of PHI in HITECH because most uses and disclosures of health data occur for 'routine' purposes, exceptions are very rare.

Congress wanted individuals to be able understand at least what, why, and to whom their health data is disclosed from electronic health records systems for the past three years.

Unless AODs are automated and include all the detailed information about all TPO uses and disclosures, individuals literally have no way to know to whom their PHI goes, or what was disclosed or used. We can't check our own PHI or get independent agents or decision support unless we can obtain robust AODs (including the copies of the PHI used or disclosed).

A market-based transition to the Triple Aim requires informed patients and competition for new patient-facing services. The essential first step for informing patients is AOD. It must be done in a way that actually engages patients through independent decision support, independent risk assessment and independent audit of all personal data uses.

Sincerely,

Deborah C. Peel, MD

Founder and Chair, **Patient Privacy Rights**
O: (512) 732-0033
www.patientprivacyrights.org