manatt

Update from the Health IT Policy Committee's Privacy and Security Workgroup

Deven McGraw, JD, MPH, LLM
Partner
Manatt, Phelps & Phillips, LLP

March 17, 2015

Background

- Health IT Policy Committee (HIT PC) = 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.
- Now known as the Privacy and Security Workgroup. New co-chair (Stan Crosley) and mostly new members.

Workgroup charge

- The Privacy and Security Workgroup will provide input and make recommendations on policy issues and opportunities to ensure that information captured and exchanged electronically is protected and shared consistent with consumer needs and expectations. The Workgroup will proactively identify topics for recommendations and be responsive to other workgroups to address privacy and security issues that are critical to workgroup deliberations. Examples of issues to be considered include, but are not limited to, topics to address interoperability goals/challenges and Big Data and privacy in healthcare.

Topics since last Summit

- Data segmentation for privacy
- Stage 3 of Meaningful Use (covered October 2013)
- Health “Big Data”
- Draft Interoperability Roadmap

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.

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.

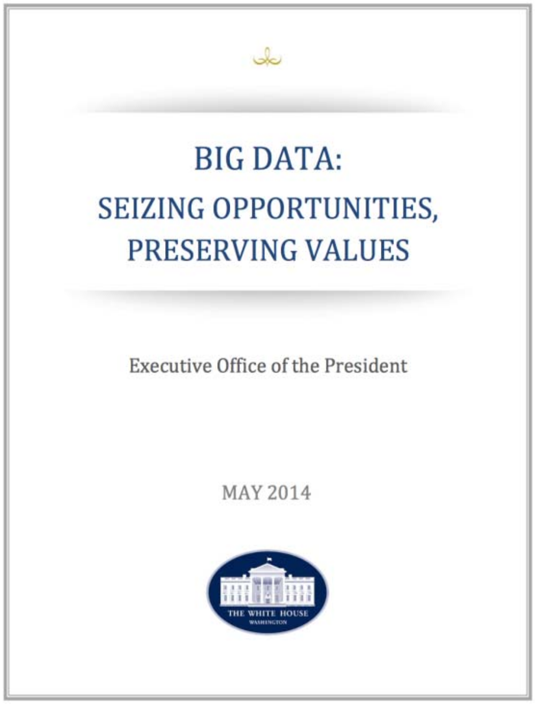
Recommendations

- 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.

White House Big Data Report: Observations



BIG DATA:
SEIZING OPPORTUNITIES,
PRESERVING VALUES

Executive Office of the President

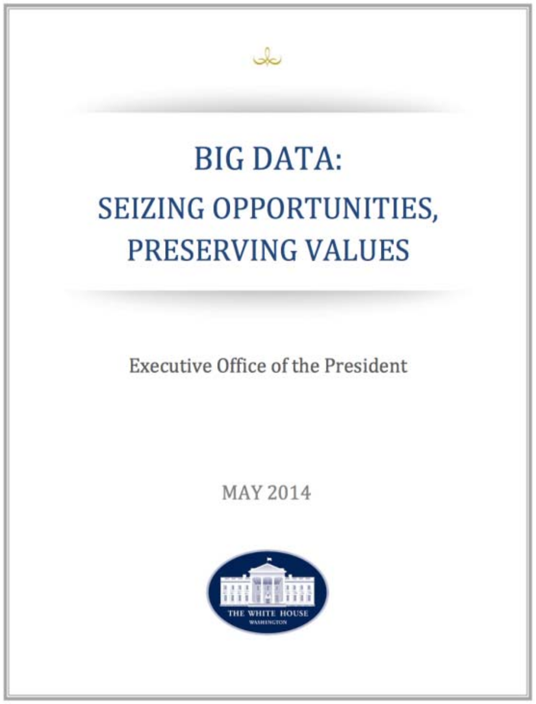
MAY 2014

White House Report (May 2014)

- Big data is characterized by 3 Vs (Volume, Variety, Velocity)
- Other key observations:
  - De-identification is insufficient to protect privacy in big data analytics
  - Meta data raises significant privacy issues
    - Should not necessarily treat as less risky than content
  - Focus on assuring responsible uses, vs. trying to control collection; role of notice and consent should be re-examined

Source: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

Why are we considering Big Data?



BIG DATA:
SEIZING OPPORTUNITIES,
PRESERVING VALUES

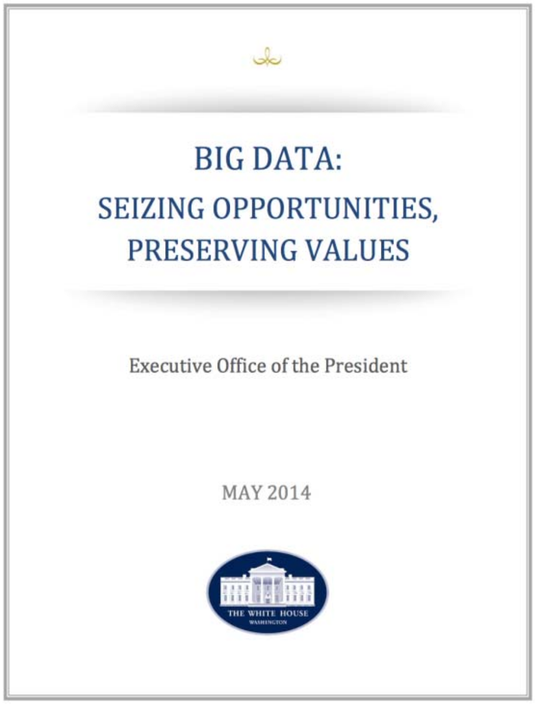
Executive Office of the President

MAY 2014

- “The government should lead a **consultative process** to **assess how** the Health Insurance Portability and Accountability Act (HIPAA) and other relevant **federal laws and regulations** can best **accommodate** the advances in **medical science and cost reduction** in health **care delivery** enabled by big data.”

Source: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

Why are we considering Big Data?



BIG DATA:

SEIZING OPPORTUNITIES,
PRESERVING VALUES

Executive Office of the President

MAY 2014

- “The complexity of complying with numerous laws when data [is] combined from various sources raises the potential need to carve out special data use authorities for the health care industry if it is to realize the potential health gains and cost reductions that could come from big data analytics.”

Source: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

Other relevant developments

- PCAST Big Data Report
- White House Open Government Partnership
- 21st Century Cures initiative
- Precision Medicine initiative
- Big Data business opportunities
  - –Venture capital in data analytics
  - –Mhealth
- Breaches

Scope of Workgroup’s inquiry

In Scope:

- Privacy and security issues – concerns and potential barriers to progress/innovation
- Potential harmful uses (related to privacy)

Out of Scope:

- Data quality/data standards
- Non-representativeness of data
  - Should not try to resolve this from the standpoint of increasing “representativeness” of data but should be considered in discussion of harmful uses

Likely Topics for Recommendations

1. Concerns about tools commonly used to protect privacy
   - **A. De-identification**
   - **B. Patient consent v. norms of use**
   - **C. Security**
   - D. Transparency
   - E. Collection/use/purpose limitations
2. Preventing/Limiting/Redressing Harms
3. Legal Landscape
   - A. Gaps or “under” regulation
   - B. “Over-” or “mis-” regulation

Public Hearing Panelists

Day 1 – December 5

Health Big Data Opportunities and the Learning Health System (LHS):

- Steve Downs, RWJF
- Richard Platt, Harvard Pilgrim
- Patricia Brennan, U. Wisconsin

Health Big Data Concerns:

- Michele DeMooy, CDT
- Mark Savage, NPWF
- Anna McCollister-Slipp, Galileo Analytics

Protections for Consumers:

- Khaled El Emam, U. of Ottawa
- Bob Gellman, Private Consultant
- Fred Cate, Indiana U.

Day 2 – December 8

Current Law:

- Melissa Bianchi, Hogan Lovells
- Kirk J. Nahra, Wiley Rein
- Deven McGraw, Manatt

Health Big Data Opportunities:

- Linda Avey, 23 and Me, Curios, Inc.
- Kald Abdallah, Project Data Sphere
- Ella Mihov, Ayasdi

Learning Health System:

- Paul Wallace, Optum Labs
- Josh Gray, AthenaHealth

Health Big Data Concerns:

- Leslie Francis, U. Utah
- Melissa Goldstein, George Washington U.

Security Testimony

- PSWG heard testimony on February 9, 2015
- 3x5 minute presentations; 45 minute discussion

Panelist	Organization	Position
Andrei Stoica	IMS Health	VP of Global Systems Development and Security
Denise Anthony	Dartmouth College	Vice Provost for Academic Initiatives, Professor of Sociology; SHARPS contributor
Ryan Andersen	Milliman	Director of Software as a Service

Questions?

Deven McGraw

Partner

Manatt, Phelps & Phillips LLP

dmcgraw@manatt.com