Health IT Policy Committee

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

Privacy and Security Workgroup

Straw Recommendations on Health Big Data

Stanley Crosley, Co-chair

June 30, 2015

Agenda

Review Straw Recommendations on Health Big Data

Health Big Data Effort to Date

- Background: White House Big Data Report* and other initiatives
- Public hearings: December 5 and 8, 2014, and February 9, 2015**
- In scope: privacy and security issues; potential harmful uses
- Out of scope: data quality/data standards; non-representativeness of data
- Post-hearing major topics:
  - Concerns about tools commonly used to protect privacy
    - De-identification, consent, security, transparency, collection/use/purpose limitation
  - Preventing, limiting, and redressing harms
  - Complex legal landscape
    - Under- and over-regulation

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

** Dec 5: http://www.healthit.gov/facas/calendar/2014/12/05/policy-privacy-security-workgroup-virtual-hearing
Dec 8: http://www.healthit.gov/facas/calendar/2014/12/08/policy-privacy-security-workgroup-virtual-hearing
Feb 9: http://www.healthit.gov/facas/calendar/2015/02/09/policy-privacy-security-workgroup

§ 5.1 - Potential for Harmful or Discriminatory Practices

- Challenges include ensuring the responsible use of big data analytics and increasing risk of harms (e.g., discrimination, harms to dignity, reduced public trust). Some US laws prohibit discriminatory uses of health data. However, other discriminatory uses of health data are not expressly prohibited by law or are expressly permitted.
- Difficult to make policy because no consensus on which uses are "harmful"; unable to predict which future uses could be harmful.
- Poor transparency can reinforce bias and unfair practices (e.g., resistance to transparency with proprietary algorithms, which are used to make decisions about people). Existence of bias may only be revealed when one understands the process used to arrive at a particular decision.

§ 6.1 - Addressing Harm, Including Discriminatory Practices

Call on effort that explores the following:

- Without a national consensus on what constitutes "harm" (beyond more obvious cases of discrimination), we encourage ONC and other federal stakeholders to promote more public inquiry to fully understand the scope of the problem – both harm to individuals and to communities.
  - E.g.: to address health insurance discrimination, Congress significantly limited health insurers' ability to use health data for insurance decisions as part of the Affordable Care Act.

§ 6.1 - Addressing Harm, Including Discriminatory Practices (cont.)

- Call on policymakers to continue to monitor the use of health big data (both health data and data used for health purposes) to identify gaps in law and regulation and areas for further inquiry .
- With respect to increasing transparency re: algorithms, consider an approach similar to that used in FCRA.
  - Any such regulation or best practice governing algorithms should aim to maximize transparency, validity, and fairness.

§ 5.2 - Different Domains of Regulation (HIPAA and "Other") Yields Contradictions and Unpredictability

- Legal complexity confuses consumers and imperils trust.
- No comprehensive, FIPPs-based protections for health data analytics in many domains.
- **Access** – individuals often lack the ability to access, use, and share own data, including research for learning health system (LHS) activities.
- **Transparency** – lack of clarity on how data is used and exchanged in big data ecosystem.
- **Research** – rules do not necessarily regulate based on privacy risk; higher hurdles for using data for research/generalizable knowledge (public good).

§ 6.2 – Address Uneven Policy Environment

- Leverage most recent recommendations by the PSWG on better educating consumers about the privacy and security laws and uses of data both within and outside of the HIPAA environment.*
- Promote FIPPs-based protections for data outside of HIPAA:
  - Voluntarily adopted self-governance codes of conduct should be encouraged, since these can be enforced by FTC if publicly declared.
  - HHS, FTC and other agencies should help guide these efforts, to help more quickly establish "rules of the road" to build trust.
  - Codes should emphasize transparency, individual access, accountability, and use limitations.

* May 22, 2015 HITPC meeting. http://www.healthit.gov/facas/sites/faca/files/HITPC_PSWG_Meeting_Slides_2015-05-22_Final.pdf

§ 6.2 – Address Uneven Policy Environment (cont.)

- Consistent with previous HITPC recommendations, policymakers should re-evaluate existing rules governing data uses that contribute to a learning health system to be sure they provide incentives for responsible re-use of data for learning purposes – for example, treating as "health care operations" learning uses of health data that are under the entity's control.* Policymakers should also consider modifying rules around research uses of data to provide incentives for the use of privacy-protecting architectures such as data enclaves.

* October 18, 2011 HITPC Transmittal Letter. http://www.healthit.gov/sites/default/files/pdf/HITPC_Privacy_and_Security_Transmittal_Letter_10_18_11.pdf

§ 6.2 – Address Uneven Policy Environment (cont.)

- Individuals should have strong rights to access their health information, sufficient to enable them to access, download, and transmit their health information as easily as they can with their financial information, either for their own use or to allow them to contribute their information for research into diseases that impact them or in any area of learning that they seek to support. This will require creating a "right of access" in entities not covered by HIPAA as part of the voluntary codes of conduct (see prior recommendation); it will also require strengthening HIPAA over time to bring it into the digital age.
- Educate consumers, health care providers, technology vendors, and other stakeholders about the limits of legal protection; reinforce the previous recommendations by the PSWG.*

* August 16, 2011 HITPC Transmittal Letter. http://www.healthit.gov/sites/faca/files/HITPC_PSTT_Transmit_8162011.pdf

§ 5.3 - De-Identification and Re-Identification

- Over-reliance on de-identification; no accountability for re-identification.
- No overarching standards for de-identification of data outside of HIPAA; HIPAA standards for de-identification often voluntary and not required.
- Concerns over both safe harbor and expert determination; no objective criteria governing expert method.
- Increased risk of re-identification when combine data sets (mosaic effect).
- De-identified data unregulated; no penalties for re-identification or negligently leaving data vulnerable.
- De-identification reduces value of data and places burden on innovation; de-identification using expert methodologies too expensive and time intensive.

§ 6.3 – Protect Health Information by Improving Trust in De-Identification Methodologies and Reducing the Risk of Re-Identification

- Call on OCR to be a better "steward" of HIPAA de-identification standards and conduct.
  - Conduct ongoing review of the methodologies and policies
  - Seek assistance from third-party experts, such as NIST
- Urge the development of initiatives or programs to objectively evaluate statistical methodologies to vet their capacity for reducing re-identification risk to "very low" in certain contexts. OCR should consider granting safe harbor status to those methodologies proven to be effective in particular contexts in order to encourage use of proven methodologies.

§ 6.3 – Protect Health Information by Improving Trust in De-Identification Methodologies and Reducing the Risk of Re-Identification (cont.)

- OCR should also consider establishing risk-based de-identification requirements in circumstances where re-identification risk has been lowered other than through treatment of the data.
  - E.g.: access to data is restricted in secure enclaves, where those holding or accessing the data have little-to-no motivation to re-identify and are prohibited from doing so in an accountable environment. Evaluate whether the context of data sharing should be part of the evaluation of re-identification risk.

§ 6.3 – Protect Health Information by Improving Trust in De-Identification Methodologies and Reducing the Risk of Re-Identification (cont.)

- PSWG desires accountability for re-identification or negligent de-identification – but recommends against specifically asking Congress to address at this time.

§ 5.4 - Security Threats and Gaps

- Silos of protections; no end-to-end secure environment for health data.
- No entity responsible for assuring end-to-end protections.
- No legal incentives for privacy-enhancing technical architectures.
- Acknowledge Congress is the only policy-making body equipped to provide a baseline level of security for health data; not calling for Congressional action at this time.

§ 6.4 – Supporting Secure Use of Data for Learning

- Urge the development of voluntary codes of conduct to address robust security safeguards that can be enforced by FTC.

- Call on public and private sectors to educate stakeholders about cybersecurity risks and recommended precautions.

- Call on policy makers to provide incentives for entities to use privacy-enhancing technologies and architectures (e.g., secure data enclaves, secure distributed data systems).

§ 6.4 – Supporting Secure Use of Data for Learning (cont.)

- Re-endorse prior Tiger Team recommendations*
  - Security policy for entities collecting, storing, and sharing electronic health information needs to be responsive to innovation and changes in the marketplace.
  - Security policy needs to be flexible and scalable.
  - Providers need education and guidance on how to comply with security policy requirements.
  - HHS should have a consistent and dynamic process for updating security policies and rapid dissemination of new rules and guidance to all affected. Call on NIST to update the NIST 800-66 Revision 1 to include a description of technology to help meet the requirements.

* 12/14/2011 HITPC Transmittal Letter. http://www.healthit.gov/sites/faca/files/hitpc_transmit_ttdec2011.pdf