DRAFT

August 5, 2015

Karen DeSalvo, MD
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. DeSalvo:

This transmittal letter presents the recommendations of the Health IT Policy Committee (HITPC) as approved on August 11, 2015.[1] These recommendations are a result of the work of the Privacy and Security Workgroup (PSWG) investigating privacy and security issues related to health big data and deliberations of the HITPC.

Broad Charge for the Privacy and Security Workgroup

In response to the White House report on big data and other complementary federal initiatives,[2,3] the PSWG was charged to investigate privacy and security issues related to big data in the healthcare space and recommend actions to address critical challenges.

The PSWG held several public meetings and hearings between October 2014 and February 2015 in which experts from industry, non-profit organizations, academia, and law were invited to present on the following issues as they relate to big data: (1) health big data opportunities, (2) health big data concerns, (3) the learning health system, (4) protections for consumers, and (5) current laws.

Background

The collection, analysis, and use of large volumes of electronic information will be a driver in the U.S. economy for the foreseeable future. Through the proliferation of software applications and mobile devices, the amount of health-related information is growing exponentially. As the volume, velocity, and variety of information continue to grow, so do the potential risks arising from unknown and inappropriate uses of protected health information (PHI).[4]

The application of big data analytics in healthcare brings opportunities to improve the health of both individuals and their communities. These benefits include safer treatments, the ability to target communities and individuals with tailored interventions, and the ability to respond to the spread of diseases more rapidly.[5] However, big data computing poses challenges to privacy and security. Rapid growth in the volume of health-related information increases the risk of privacy violations,[6] particularly

[1] http://healthit.gov/FACAS/health-it-policy-committee/hitpc-workgroups/privacy-and-security-workgroup
[2] Big Data: Seizing Opportunities, Preserving Values, May 2014, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[3] https://www.whitehouse.gov/the-press-office/2014/09/24/fact-sheet-announcing-new-us-open-government-commitments-third-anniversa
[4] Protected Health Information is defined in 45 CFR § 160.103.
[5] Public Hearing Responses of Richard Platt, p. 3, http://www.healthit.gov/facas/sites/faca/files/PSWG_Background_Richard_Platt_Reply_to_Questions_for_Panelists_2014-12-05.pdf.
[6] Michelle De Mooy, Privacy and Security Workgroup Transcript, December 5, 2014, p. 30 [hereinafter "December 5"].

when data sets are combined.[7] Data anonymization tools such as de-identification are useful, but cannot eliminate risks of re-identification.[8]

Below is a high-level summary of the Workgroup's recommendations.

Recommendations:

1) Address Harm, Including Discrimination Concerns

a) Encourage ONC and other federal stakeholders to promote more public inquiry to understand the full scope of the problem – both harm to individuals and communities.
b) Policymakers should continue focusing on identifying gaps in legal protections against what are likely to be an evolving set of harms from big data analytics.
c) Policymakers should adopt measures that could increase transparency about actual health information uses.
d) Policymakers should explore how to increase transparency around use of the algorithms used in big health analytics, perhaps with an approach similar to that used in the Fair Credit Reporting Act (FCRA).

2) Address Uneven Policy Environment

a) Promote Fair Information Practice Principles (FIPPs)-based protections for data outside of HIPAA:
    i) Voluntarily adopted self-governance codes of conduct. In order to credibly meet the requirements of both protecting sensitive personal information and enabling its appropriate use, Codes must include transparency, individual access, accountability, and use limitations.
    ii) U.S. Department of Health and Human Services (HHS), Federal Trade Commission (FTC), and other relevant federal agencies should help guide such efforts to more quickly establish dependable "rules of the road" and to ensure their enforceability in order to build trust in the use of health big data.
b) Policymakers should evaluate existing laws, regulations, and policies (rules) governing uses of data that could contribute to a LHS to assure those rules promote responsible re-use of data to contribute to generalizable knowledge.
c) Policymakers should modify rules around research uses of data to incentivize entities to use more privacy protecting architectures, for example by providing safe harbors for certain behaviors and levels of security.
d) To support individual's rights to access their health information, create a "right of access" in entities not covered by HIPAA as part of the voluntary codes of conduct; also revise HIPAA over time to enable it to be effective at protecting health data in the digital age.
e) Educate consumers, healthcare providers, technology vendors, and other stakeholders about the limits of legal protection; reinforce previous PSWG recommendations.
    i) Leverage most recent PSWG recommendations on better educating consumers about privacy and security laws and uses of personal information both within and outside of the HIPAA environment.

[7] Lucia Savage, December 5, p. 24.
[8] Michelle De Mooy, December 5, p. 30.

3) Protect Health Information by Improving Trust in De-Identification Methodologies and Reducing the Risk of Re-Identification

a) The Office for Civil Rights (OCR) should be a more active "steward" of HIPAA de-identification standards.
   i) Conduct ongoing review of methodologies to determine robustness and recommend updates to methodologies and policies.
   ii) Seek assistance from third-party experts, such as the National Institute of Standards and Technology (NIST).
b) Urge development of initiatives or programs to objectively evaluate statistical methodologies to vet their capacity for reducing risk of re-identification to "very low" in particular contexts.
c) OCR should grant safe harbor status to methodologies that are proven to be effective at de-identification in certain contexts to encourage use of proven methodologies.
d) OCR should establish risk-based de-identification requirements in circumstances where re-identification risk has been lowered.

4) Support Secure Use of Data for Learning

a) Urge development of voluntary codes of conduct that also address robust security provisions.
b) Policymakers should provide incentives for entities to use privacy-enhancing technologies and privacy-protecting technical architectures.
c) Public and private sector organizations should educate stakeholders about cybersecurity risks and recommended precautions.
d) Leverage recommendations made by the Privacy and Security Tiger Team and endorsed by the HITPC in 2011[9] with respect to the HIPAA Security Rule.

Please see Appendix A for the full report.

We appreciate the opportunity to provide these recommendations and look forward to discussing next steps.

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee

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