NCVHS

Health Information Privacy and Security Beyond HIPAA

Background

NCVHS is charged with studying and identifying "privacy and security and access measures to protect individually identifiable health information in an environment of electronic networking and multiple uses of data." To that end, it has advised the Secretary on matters relating to the implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) over the past two decades. HIPAA establishes a regulatory framework for managing and using personally identifiable health information by covered entities and business associates.

The challenges, however, of protecting privacy using even de-identified information are far greater today than when the HIPAA privacy and security rules went into effect. Uses for increasingly complex data are growing exponentially as new powerful tools are able to combine data sets and extract information from large volumes of data. Advancing interoperability creates new challenges, as does meaningful engagement of consumers, families and communities in advancing health and health care. Privacy and security are linked to all the ways in which information about individuals is collected, analyzed, and used in our increasingly digital society.

NCVHS has been recommending privacy and security stewardship frameworks and guidance extending beyond HIPAA covered entities and business associates for over a decade. For example, the 2008 report for policy makers, *Enhancing Protections for Uses of Health Data: A Stewardship* calls on any person or entity that "collects, views, stores, exchanges, aggregates, analyzes, and/or uses electronic health data to practice sound data stewardship. In 2012, NCVHS recommended *A Stewardship Framework for the Use of Community Health Data.* Recently, NCVHS addressed current issues in de-identification of health information for a growing range of uses. The Office of the National Coordinator for Health IT and the Office for Civil Rights have contributed to policy and guidance for those who access or use health information but are not covered entities or business associates.

Goals

Building on past work, this project will take a more comprehensive look at a range of challenges beyond HIPAA and the range of policy options that may be available to the Department, to data stewards, and to the subjects of the information. Specific goals are as follows:

1. Identify and describe the changing environment and the risks to privacy and security of confidential health information; highlight promising policies, practices and technology,
2. Lay out integrative models for how best to protect individuals' privacy and secure health data uses outside of HIPAA protections while enabling useful uses, services and research,
3. Formulate recommendations for the Secretary on actions that HHS and other federal Departments might take, and
4. Prepare a report for health data stewards.

Plan

The project will be carried out in four phases, each informing the work of the next phase.

Phase I –Conduct an environmental scan to explore key drivers of health information privacy and security challenges beyond the scope of HIPAA. The scan will explore existing and emerging policy frameworks, practices and technologies to better frame key issues and drivers of change in the following areas.

1. Big data and expanding uses and users
2. Cyber-security threats and approaches
3. Evolving technologies for privacy and security
4. Laws in other domains (e.g. Fair Credit Reporting restricting uses of consumer data)
5. Evolving consumer attitudes
6. Personal devices and internet of things

In some areas, the process of environmental scan may also identify emerging solutions. The environmental scan will be accomplished through hearings and background research and study to learn from a range of federal agencies, from academics, technologists, and thought leaders, including current thinking and approaches of other countries.

Approach: One or more hearings, background research. Participants may include representatives from federal sources (CMS, ASPE, ONC, OCR, FTC) and private sector stakeholders including consumers, academics, CIOs, technologists, and thought leaders.

Deliverable: A report of environmental scan findings.

Phase II – Based on what is learned in the environmental scan, develop models and illustrative future scenarios, laying out assumptions and identifying areas of uncertainty. This is reflective work that the committee and invited advisors will undertake to develop integrative models for how best to protect individuals' privacy and secure health data uses outside of HIPAA protections while enabling uses, services and research.

Approach: Invitational roundtable to develop models and scenarios and identify potential policy, practice and technology solutions.

Deliverable: A report describing a policy framework including benefits, levers, and relationships of policy alternatives.

Phase III - Prepare recommendations for the Secretary of HHS that may include:

- A framework of guiding principles to advance governance of health information and inform how to navigate the changing landscape beyond HIPAA,
- Privacy and security policy and standards across federal agencies and states,
- Levers that HHS can apply such as Quality Payment Programs, data release best practices, education and guidance, and

- Legislative mechanisms such as fines for unauthorized or misuse of health information.

Approach: Depending on clarity of the policy framework coming out of Phase II, hold an additional hearing to discuss alternatives or go directly to preparation of a letter for the Secretary.

Deliverable: Letter to the Secretary to be drafted and approved by the NCVHS.

Phase IV – Prepare a report for the health care industry and data stewards and users of health data reflecting a framework and policy and practice recommendations. This would be modeled on the earlier Stewardship Primer.

Approach: Report, primer or toolkit

Timeframe

	2018 – Q 1 & 2	2018 – Q 3 & 4	2019 – Q 1 & Q 2	2019 – Q 3 & 4
Phase I: This phase will be accomplished by holding one or two two-day hearings including one or more panels on each of the five topics areas.	**X**			
Phase II: This phase will be accomplished by hosting a roundtable to deliberate findings from the environmental scan.		**X**		
Phase III: This phase consists of preparing and approving a letter to the HHS Secretary.			**X**	
Phase IV: This phase will turn the learning and recommendations into a framework or toolkit for those who handle health data but are not subject to HIPAA.				**X**

NCVHS Reports on Privacy and Security-related Issues since 1996

1997

- June 27, 1997 Letter to the Secretary with Recommendations on Health Privacy and Confidentiality
- September 9, 1997, Letter to the Secretary with Recommendations on Security Standards to Protect Health Care Information
- June 23, 1998, Letter to the Secretary with Findings of the Subcommittee on Privacy and Confidentiality Concerning Identifiability of Health Information and Confidentiality Considerations for Health Registries

2000

- February 7, 2000 Recommendations on the notice of proposed rule-making for standards for privacy of individually identifiable health information

2001

- October 1, 2001 Letter to the Secretary on Consent Requirements and Minimum Necessary Provisions as it relates to the new Privacy Rule
- November 21, 2001 Letter to the Secretary on Research recommendations as it relates to the new Privacy Rule

2002

- April 25, 2002 Letter to the Secretary – Privacy and Confidentiality Additional Recommendations and Response to NPRM
- March 1, 2002 Letter to the Secretary – Privacy and Confidentiality Recommendations on Marketing and Fundraising
- November 25, 2002 Letter to the Secretary – regarding comments on the implementation of Privacy & Confidentiality regulations
- September 27, 2002 Letter to the Secretary – Comments on Preparations for Implementation of Privacy and Confidentiality regulations

2003

- March 5, 2004 – Letter to the Secretary – Recommendation on the effect of the Privacy Rule

2004

- June 17, 2004 – Letter to the Secretary – Recommendations on the Effect of the Privacy Rule in Law Enforcement
- June 17, 2004 – Letter to the Secretary – Recommendations on the Effect of the Privacy Rule in Schools
- June 17, 2004 – Letter to the Secretary – Recommendations on the Effect of the Privacy Rule in Banking

- September 2, 2004 – Letter to the Secretary – Findings and Recommendations on the Impact of the Privacy Rule on Fundraising

2005

- September 9, 2005 – Letter report to the Secretary – on Personal Health Record (PHR) systems

2006

- June 22, 2006 – Letter to the Secretary – Recommendations regarding Privacy and Confidentiality in the Nationwide Health Information Network

2007

- June 21, 2007 – Letter to the Secretary – Update to privacy laws and regulations required to accommodate NHIN data sharing practices
- December 22, 2007 – Report to the Secretary – Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data

2008

- February 20, 2008 – Letter to the Secretary – Individual control of sensitive health information accessible via the Nationwide Health Information Network for purposes of treatment
- April 24, 2008 – Enhancing Protections for Uses of Health Data: A Stewardship Framework

2009

- July 1, 2009 – Report to the Secretary – Recommendations on Privacy and Confidentiality, 2006-2008
- September 2009 – Health Data Stewardship: An NCVHS Primer
- September 28, 2009 – Letter to the Secretary – Protection of the Privacy and Security of Individual Health Information in Personal Health Records

2010

- November 10, 2010 – Letter to the Secretary – Recommendations Regarding Sensitive Health Information

2012

- December 5, 2012 – Letter to the Secretary – A Stewardship Framework for the Use of Community Health Data

2015

- May 2015 – Report – Toolkit for Communities Using Health Data: How to collect, use, protect, and share data responsibly
- September 16, 2015 – Letter to the Secretary – Recommendations on the financial services industry and § 1179 of HIPAA

2016

- November 9, 2016 – Letter to the Secretary – Recommendation on the HIPAA Minimum Necessary Standard

2017

- February 23, 2017 – Letter to the Secretary – Recommendations on De-identification of Protected Health Information under HIPAA