National Committee on Vital and Health Statistics
Advising the HHS Secretary on National Health Information Policy

Beyond HIPAA:

Registries as an exemplar of health data "Beyond HIPAA"

Privacy, Confidentiality & Security Subcommittee

May 15, 2018

Beyond HIPAA Initiative

Builds on NCVHS's past work and the work of other government and private initiatives to consider a health data privacy and security framework for 21st century health information challenges.

Goals:

- Identify and describe the changing environment and the risks to privacy and security of confidential health information; highlight promising policies, practices and technology;
- 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;
- Formulate recommendations for the Secretary on actions that HHS and other federal Departments might take; and
- Prepare a report for health data stewards.

Environmental Scan* Findings

1. Health information lives in two worlds: one is regulated by HIPAA and the other is unregulated and not subject to HIPAA or, for the most part, any other statutory regulation for privacy.

2. HIPAA minimizes health information definitional issues, but clarity dissolves as information passes beyond HIPAA protections. Among the many examples discussed:
   - Data in the hands of a registry is subject to variable and incomplete privacy policies and has uneven legal protections.
   - New technologies that enable patients to generate data outside of clinical settings and share it with providers are not subject to a consistent legal and regulatory framework and pose integrity, security breaches, malware, and privacy issues.

3. Giving consumers a greater say in the use of their health data is far more difficult in the unregulated world.

4. Mechanisms such as sequestering privacy sensitive data and de-identifying data, are helpful but not sufficient.

5. HIPAA and other privacy regulations including the EU General Data Protection Regulation are built on the Fair Information Practice Principles.

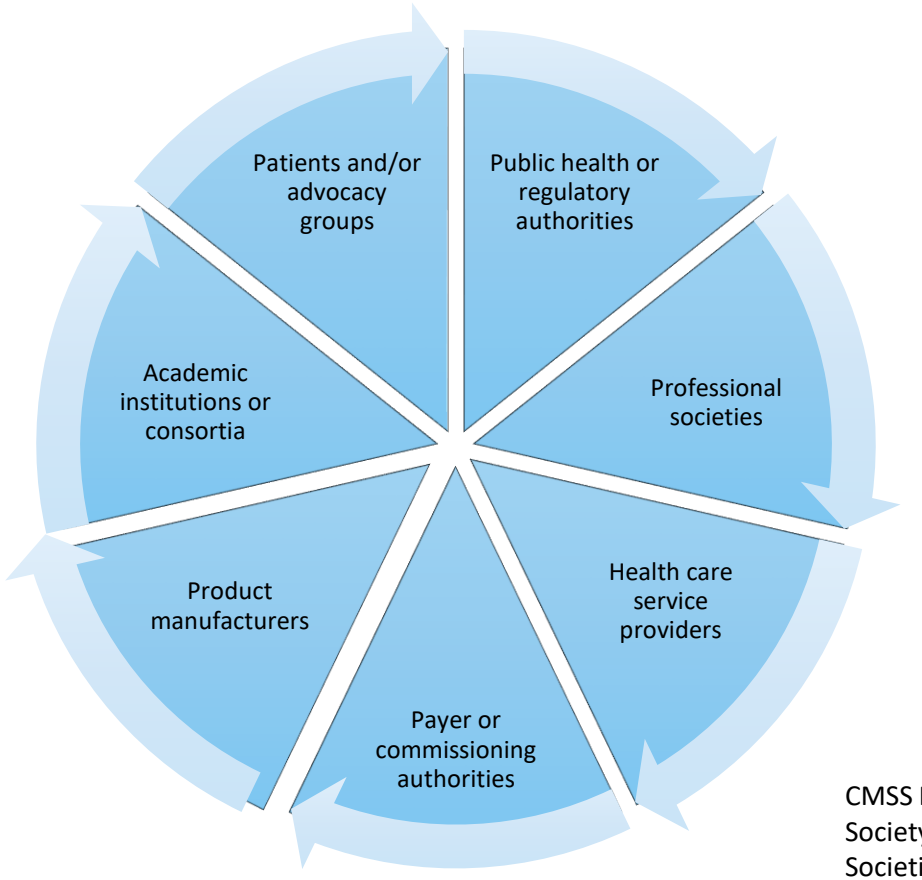
6. Consumer attitudes continue to evolve and may have evolved more quickly of late in response to greater exposure to Facebook and Google business practices.

*NCVHS. Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges. https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf

Health Registry as Exemplars

- Best practices models: registries that have voluntarily adopted sound governance and operations to protect the privacy and security of information.
- Guiding organizations: Private sector organizations to convene registry stakeholders. Active research, policy and education programming.
- Federal stake in registries for quality measurement and research.
- Robust literature and authoritative reports aimed at advancing the industry.

Registry Sponsors



CMSS Primer for the Development and Maturation of Specialty Society Clinical Data Registries; Council of Medical Specialty Societies, January 2016: https://cmss.org/wp-content/uploads/2016/02/CMSS_Registry_Primer_1.2.pdf

1. In the context of health data registries, discuss the problems arising from processing of Personally Identifiable Information (PII)*

Problems	Examples	Likelihood
Loss of Trust		
Loss of Self Determination (Physical harm, loss of autonomy, loss of liberty, exclusion		
Discrimination (stigmatization, power imbalance)		
Economic Loss		

NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems
https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

2. In the context of health data registries, consider the pros and cons of the following models. Are there others? How might the Committee go about evaluating the efficacy of each general approach?

General models for PII	Description
1. Extend existing laws and associated regulation	Extend the boundaries of HIPAA to cover certain uses; extend the definition of a business associate; entity extend the regulatory authority of FTC
2. Mandatory PHI data use agreement	Formalized agreement for any disclosure of PHI (and de-identified data?)
3. Data protection model	Similar to the new EU General Data Protection Law establishing the rights of individuals and the obligations of data processors and holders.
4. Mechanism to certify or accredit organizations to PHI and de-identified datasets are disclosed.	Evaluate privacy and security policy and processes of recipients of datasets.

3. Please comment on the project plan for assessing models

- Outreach to key registry experts to further develop models and identify best practice examples.
- Lay out a stewardship framework and integrative model for how best to protect individuals' privacy and secure health data in registries while enabling useful uses, services and research,
- Identify actions that registry sponsors can take to better safeguard privacy
- Identify potential recommendations for the Secretary on actions that HHS and other federal Departments might take.

4. What other resources, experts should the Committee confer with during this phase of its Beyond HIPAA work?

September 2018

1. Repeat this discussion focusing on personal health devices
2. Come out of September meeting with a plan for moving forward with Beyond HIPAA
   - Roundtable to work on models?
   - Further hearings?
   - Additional exemplars?
   - Letter to Secretary?