Ongoing and Emerging Issues in Privacy and Security in a Post-Covid-19 Era: An Environmental Scan

Cason D. Schmit
Assistant Professor
Director, Program in Health Law and Policy
Dept. Health Policy & Management
School of Public Health, Texas A&M University

December 7, 2022

ATM | TEXAS A&M UNIVERSITY®

FEARLESS ON EVERY FRONT

NCVHS & Subcommittee on Privacy, Confidentiality and Security (PCS)

NCVHS assists and advises the Secretary on health data, statistics, privacy, national health information policy, and the Department's strategy to best address those issues.

The PCS Subcommittee commissioned a brief environmental scan of recent privacy, confidentiality and security issues in the health, healthcare, and/or public health sector to guide the PCS Subcommittee and full Committee in identifying new major projects to pursue.

Disclaimer

- This environmental scan was completed on an extremely tight timeline, and it should not be considered a comprehensive overview of all developments in privacy, confidentiality, and security since 2018. Issues that were not covered in the environmental scan but are included in this presentation will be highlighted in **red**.

Environmental Scan Outline

Executive Summary

I. Introduction & Background

II. Significant Changes in the Privacy Landscape Since 2018

III. New Privacy and Security Rules

IV. Promising Policies, Practices, and Technologies

V. Potential Problems in Governance of Health Information

VI. Opportunities for Timely Advice from NCVHS to the HHS Secretary Regarding Constructive Actions that HHS and Other Federal Departments Might Take

VII. References

Presentation Overview

- Significant Changes in the Privacy Landscape Since 2018
  - FTC ANPR on Commercial Surveillance*
  - Common Rule definitions for “identifiable”*
- Alternative Approaches to Privacy and Enforcement
- De-identification*
- Artificial Intelligence*
- Increasing Privacy Threats
  - Law Enforcement Use of Health Data*

* Indicates potential NCVHS opportunity for timely advice to HHS

Report Highlight:

Significant Changes in the Privacy Landscape Since 2018

State Policy Developments

- State Privacy Laws Enacted
  - CA, CO, CT, VA, UT
- Overview of State Privacy Laws Under Consideration
  - 49 inactive bills in 4 states
  - 4 states with active bills: MI, NJ, OH, PA
- Other State Law Proposals
  - Uniform Personal Data Protection Act introduced in 3 jurisdictions
  - Bills on artificial intelligence (AL, CO, IL), biometric data (IL, TX, WA)

Federal Policy Developments

- Federal Privacy Laws Enacted
  - 21st Century Cures Act regulations on “information blocking”
  - Common Rule revision (2017) became effective in 2018
- Federal Privacy Laws Under Consideration
  - American Data Privacy and Protection Act
  - FTC Advance Notice of Proposed Rulemaking (APRN) on “commercial surveillance and data security.”
  - Common Rule agencies currently “reexamining” the meaning of “identifiable private information”
  - FDA Draft Guidance on Cybersecurity in Medical Devices (2018, 2022)

Report Highlight:

FTC ANPR on Commercial Surveillance

FTC ANPR on Commercial Surveillance

- ANPR status
  - Public comments closed on Nov. 21, 2022
  - FTC will review comments and decide whether it will proceed with a rulemaking process, which requires:
    - Notice of Proposed Rulemaking (NPR), including proposed regulation text
    - Public comment period
    - Final Rule (challenges to any final rule are likely)
- FTC has broad jurisdiction that includes HIPAA covered entities
  - Future rules could create compliance confusion or have unintended impacts on beneficial data practices, including healthcare and public health applications

Potential NCVHS Opportunity for Timely Advice to HHS

FTC ANPR on Commercial Surveillance

Potential NCVHS Opportunity for Timely Advice to HHS: FTC ANPR on Commercial Surveillance

- Early collaboration between HHS and FTC can mitigate unintended consequences

- Potential topics for input:
  - Beneficial data practices that could be impeded by future FTC rules
    - E.g., Learning health systems, precision public health, and private sector assistance in public health surveillance.
  - Harmful health-related data practices
  - Conflicts with existing privacy frameworks like HIPAA
  - Group harms

Potential NCVHS Opportunity for Timely Advice to HHS

Common Rule definitions of “identifiable”

Potential NCVHS Opportunity for Timely Advice to HHS: Common Rule definitions of "identifiable"

- 45 C.F.R. §46.102 (e)(7): Common Rule agencies "shall"
  - Reexamine the legal definitions of "identifiable" private information" and "identifiable biospecimen"
    - "within 1 year and regularly thereafter (at least every 4 years)"
  - **Agencies may alter legal interpretations if "appropriate and permitted by law"**
  - Common Rule agencies also required to assess analytic technologies or techniques that can generate "identifiable" private information or biospecimens
- **Any input would be timely, including recommending no changes**

Report Highlight:

Alternative Approaches to Privacy and Enforcement

Approaches to Privacy and Data Protection

- **Consumer protection approach**
  - Protection through consumer rights (e.g., notice and consent)
- **Data protection approach**
  - Principle-based protections (e.g., purpose limitation, minimization)
  - Protections that "follow the data"
- **Antitrust approach**
  - Focusing oversight on entities of sufficient size as defined by law
- **Information fiduciary approach**
  - Imposing duties of confidentiality, loyalty, and care on controllers/processors

Enforcement Approaches

- **Traditional enforcement approaches**
  - Governmental agency enforcement (e.g., empower existing agency, create new agency)
  - Individual right of action (e.g., right to sue, class actions)
- **Enforcement alternatives**
  - Deputize intermediaries to enforce standards
  - Scale legal standards and penalties with the scope of data activities
  - Profit disgorgement
  - Personal liability for executives

Report Highlight:

De-identification

Report Highlights: De-identification

- Deidentification
  - Legal mechanism
  - Ethical protection

- Rapidly changing environment challenges existing guidance (2012)
  - "Arms race" between deidentification and reidentification techniques

- Unintended consequences
  - Group harms and "data genocide"

NCVHS Recommendations in 2017 on De-identification of Protected Health Information under HIPAA

- NCVHS Subcommittee on Privacy, Confidentiality and Security held a hearing in May 2016
- Committee **issued 12 recommendations to the HHS Secretary** on De-identification of Protected Health Information under HIPAA in February 2017
  - **Recommendations did not include suggestion to update/change the standard**
  - Online at: https://ncvhs.hhs.gov/wp-content/uploads/2018/03/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf

NCVHS 2017 De-identification Recommendations

	Recommendations
R1	Reinforce the current standard with sub-regulatory guidance and the other actions
R2	Develop guidance on how mechanisms (e.g., DUAs, authorization, encryption, etc.), are used to bolster the management of de-identified data
R3	Establish an information clearinghouse of de-identification best practices
R4	Develop a written competency guide for practitioners responsible for de-identification.
R5	Provide guidance on policies and practices for management and disclosure of de-identified data and for assessing risks (i.e., re-identification, individuals and vulnerable populations).
R6	Define the minimal skills and competencies to be considered a de-identification “expert”
R7	Require that CEs and BAs maintain a description of the de-identification method, the assumptions used in re-identification risk assessment, and the results of the risk assessment.
R8	Use Model Notice of Privacy Practices to inform individuals about de-identified data and its uses
R9	Define and promulgate the responsibilities of recipients of de-identified data sets.
R10	Establish a reporting process for public concerns about re-identification
R11	Investigate the feasibility of requiring CEs and BAs to track disclosures of de-identified and limited data sets
R12	Support a research agenda on de-identification methods and on re-identification.

Potential NCVHS Opportunity for Timely Advice to HHS

De-identification

Potential NCVHS Opportunity for Timely Advice to HHS: De-identification

- Not clear that subsequent actions on 2017 recommendations have been taken
- Many recommendations are still relevant
- Existing operational and technical guidance on deidentification is increasingly out of date.
- NCVHS might consider exploring considerations of both individual and group harms related to methodological approaches in data aggregation and de-identification

Report Highlight:

Artificial Intelligence

Report Highlights: Artificial Intelligence

- Rapid technological advancements make a moving regulatory target
- Transparency for public, regulators, developers, and users
- Ubiquity of AI raises legitimate concerns of structural inequities
- Group harms
  - **Comprehensible Groups**
    - Legally protected (e.g., sex, race, religion)
    - Not protected (e.g., dog owners, video game players)
  - **Incomprehensible Groups**
    - E.g., mouse movements, click patterns

Report Updates for AI

- White House: Blueprint for an AI Bill of Rights (Oct. 2022)
  - Principles:
    - Safe and Effective Systems
    - Algorithmic Discrimination Protections
    - Data Privacy
    - Notice and Explanation
    - Human Alternatives, Consideration, and Fallback
- NIST: Draft AI Risk Management Framework
  - Comments closed Oct 2022
  - Intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.

Potential NCVHS Opportunity for Timely Advice to HHS

Artificial Intelligence

Potential NCVHS Opportunity for Timely Advice to HHS: Artificial Intelligence

- **Federal laws do not distinguish between automated and traditional manual data uses and practices.**
  - However, the risks are different in scope and scale
- **A future NCVHS convening could explore:**
  - Standards and requirements for algorithmic impact assessments (e.g., unlawful discrimination, inequitable impact, group harms)
  - Standards and requirements for AI transparency
  - Scaling standards, duties, or penalties based on the size and sophistication of the data controller.

Report Highlight:

Increasing Privacy Threats

Report Highlights: Increasing Privacy Threats

- Law enforcement
  - ▫ Balancing benefits and harms of law enforcement disclosure provisions
  - ▫ Increasing use of private databases for law enforcement
    - Commercial genetic databases
    - Commercial surveillance data purchased from data brokers
- New risks post *Roe v. Wade*
  - ▫ The Supreme Court decisions in *Dobbs v. Jackson* permitted states to investigate and prosecute legal violations relating to abortion
    - Includes use of HIPAA data, non-HIPAA data, and health-adjacent data
- Concerns other privacy rights could be at risk (e.g., birth control)
  - ▫ President Biden is expected to sign a new bill protecting same-sex and interracial marriages

Potential NCVHS Opportunity for Timely Advice to HHS

Law Enforcement Use of Health Data

Potential NCVHS Opportunity for Timely Advice to HHS: Law Enforcement Access to Health Records

- Drawing the line between appropriate and inappropriate law enforcement uses of health data could be quite challenging.
- Some issues could be explored in more detail include,
  - Narrowing the scope of the HIPAA law enforcement exception
  - Imposing data protection requirements on data disclosed for law enforcement purposes (e.g., data minimization, purpose limitations).
  - Imposing higher legal standards and restrictions for generalized (as opposed to individualized) law enforcement data requests.

Discussion

schmit@tamu.edu