Shifting Privacy Laws and Health Data: An Overview

Graham Dufault
ACT | The App Association & The Connected Health Initiative
Outline

▶ Current Federal Law
  – Health Insurance Portability and Accountability Act (HIPAA)
  – Federal Trade Commission (FTC) Act
▶ State Privacy Laws / Proposals
  – California
  – Washington
▶ U.S. Law compared to Europe’s General Data Protection Regulation (GDPR)
▶ Federal Proposals
  – Healthcare privacy bills
  – General privacy bills
Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA, 45 CFR 160, 162, and 164
  - Scope: Limited to “covered entities” and “business associates” (CEs and BAs)
    - CEs include providers that process insurance claims and “health plans”
    - BAs include “vendors” that contract w/ CEs and process Protected Health Information on behalf of CEs. BAs are required to comply w/ HIPAA via contracts w/ CEs, but can also be subject to penalties directly from the agency (Office of Civil Rights or OCR)
  - Privacy Rule: Generally, HIPAA prohibits CEs and BAs from using or disclosing PHI except as expressly permitted by the patient to which it pertains or if the data has been “deidentified”
  - Security Rule: Requires appropriate administrative, physical and technical safeguards to ensure confidentiality, integrity, and security of electronic PHI
HHS Information Blocking Rule

  - To support the “access, exchange, and use of electronic health information (EHI)”
  - Requires EHR companies, other entities under HHS jurisdiction to make EHI available upon patient request to “third-party” entities including healthcare apps outside HIPAA jurisdiction (not BAs or CEs)
  - What about privacy and security?
    • Upon request via a patient to share EHI w/ third party, may communicate w/ the patient as to the risks around privacy and security and clarify that they are not responsible for an app’s privacy & security practices w/ respect to EHI
    • May request attestation as to the security and privacy practices
    • Disclosure to the patient helps the Federal Trade Commission (primary federal enforcer) police the activities of health apps outside HIPAA umbrella
Section 5 deals with antitrust and consumer protection. The consumer protection “half” prohibits:

- Unfair or
- Deceptive
- Acts or
- Practices
- In or affecting commerce 15 USC 45(a)
  - Shorthand: UDAP

Generally, no civil penalty authority – a typical complaint results in settlement.

- Ex. – Flo app (Jan. 13, 2021). A period and fertility tracking app w/ 100 mn users said health data would be kept confidential but shared that data with third party analytics providers.
  - Settlement: independent review of privacy, must get consent for sharing. Violation of agrmt triggers up to $43,792 per record penalty.
  - FTC voted 5-0 but partial dissent points out: FTC never enforced Health Breach Notification Rule.
Federal Trade Commission Act (cont’d)

- No rulemaking except under “Magnuson-Moss Act” procedures
- Or as specifically authorized by Congress using Administrative Procedure Act procedures (the typical federal rulemaking process)
  - Health Breach Notification Rule – 16 CFR 318 - Requires vendors of “personal health records and related entities” to notify consumers following a breach involving unsecured information “without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.” 16 CFR 318.4(a).
    - Never been enforced, but incoming Democratic majority likely to try to make use of it, based on dissent in *Flo*.
- FTC also has two relevant guides urging digital health companies to examine requirements of Health Breach Notification rule and which laws apply:
  - [Mobile Health App Developers: FTC Best Practices](#)
  - [Developing a Mobile Health App?](#)

ACT | The App Association
California Consumer Privacy Act

- CCPA is first comprehensive state privacy law of general applicability

- The primary health data privacy law in CA is California Confidentiality of Medical Information Act (CMIA, Cal. Civ. Code 56 et seq.)
  - CMIA is a “mini-HIPAA;” not in conflict w/ HIPAA and HIPAA doesn’t preempt CMIA

- When does CCPA apply to healthcare data processing?
  - “Patient information” (PHI) of HIPAA CEs / BAs and CMIA providers of health care is not subject to CCPA
    - However, non-PHI like website browsing, advertising data is subject to CCPA
  - Initially, CCPA defined “deidentified information” differently from HIPAA, causing confusion, but cleared up later with California Privacy Rights Act
California Consumer Privacy Act (cont’d)

- California Privacy Rights Act (CPRA) – enforceable July 1, 2023
  - Cal. Civ. Code 1798.146(a)(4) – clarifies exemption for deidentified information to if deidentification is performed in accordance w/ HIPAA
    - CPRA Requires companies to publicly commit to maintaining and using information only in deidentified form and to contractually obligate any recipients of information to do the same
  - Adds definition of “sensitive personal information,” including personal information “collected and analyzed concerning a consumer’s health” outside the scope of HIPAA and CMIA
Anonymized and Deidentified Data

- HIPAA: Deidentified data is not “individually identifiable,” so it is not subject to HIPAA protections
  - HIPAA allows two deidentification methods (45 CFR 164.514):
    - **The statistical method:**
      - Qualified expert
      - Using accepted statistical methods
      - Determines only a small chance that info could be used, alone or in combination w/ other reasonably available info
      - By an anticipated recipient to identify an individual
Anonymized and Deidentified Data (cont’d)

• **The Safe Harbor Method:**
  – All 18 listed identifiers (including name, address, zip codes, dates less than a year) must be removed from the dataset

➤ **Use in practice**
  – Researchers typically use statistical method
    • Need to link records related to individual patient across multiple health care providers or plans
  – Increasingly difficult to meet *statistical method* standard:
    • Risk of reidentification increases given proliferation of comprehensive datasets about individuals, esp. those held by larger tech firms that are performing analytics for covered entities
    • No private right of action in HIPAA, but noncompliance w/ HIPAA is std of care
Washington Privacy Act (SB 5062)

- Exempts PHI “for the purposes of [HIPAA]” (Sec. 102(2)(i))
- Exempts “healthcare information” for purposes of Washington state health privacy law, chapter 70.02 Rev. Code Wash.
- For private sector firms w/ exposure notification / contact tracing technology – unlawful for a controller or processor to:
  - Process covered data for a covered purpose unless they provide a consumer with the required privacy notice and obtain consumer consent;
  - Disclose covered data to federal, state, or local law enforcement;
  - Sell any covered data; or
  - Share covered data with another controller, processor, or third party unless such sharing is covered by contract
Europe: General Data Protection Regulation (GDPR)

- **Scope**: Global; applies to any entity processing data on EU subject, w/ exceptions
  - Covers healthcare data and healthcare entities; not divided like U.S. federal privacy law
- **Data Subject Rights**
  - Right to transparency (Art. 12)
  - Right to access (Art. 13 - 15)
  - Right to rectify inaccuracies (Art. 16)
  - Right to be forgotten (Art. 17)
  - Right to restriction of processing (Art. 18)
  - Right to object (Art. 21)
  - Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects him or her (Art. 22)
GDPR (cont’d)

- **Lawful bases for processing:**
  - Consent (explicit, for one or more specified purposes, given after clearly communicated choice, not required to conclude another contract)
  - Legitimate interest:
    - Furthers a legitimate interest
    - Processing necessary for that purpose
    - Individual’s interests do not override legitimate interest in processing
  - Performance of a contract
  - Legal obligation
  - Public task (gov’t agencies)
  - Vital interests of individual (necessary to protect life; *not* healthcare data)
Processing healthcare data is prohibited unless one of the following apply:

- Data subject gives “explicit consent”
  - “unambiguous” versus “explicit” – not clear what additional requirements this imposes but generally means strongest forms of agreement
- “Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services”
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices”
Congress – Healthcare Privacy bills

Protecting Personal Health Data Act (S. 1842, 116th) – Sens. Klobuchar / Murkowski
- Extends HHS’ / ONC’s jurisdiction, requiring HHS to promulgate regulations based on recommendations from National Task Force on Health Data Protection
  - Creates the Task Force, rules due 6 months after recommendations issued
  - Recommendations must comment on uniform standards for
    - user consent,
    - secondary uses outside primary purpose,
    - a process to permit withdrawal of consent,
    - right to access,
    - right to delete
  - What about HIPAA? Clarifies applicability only to non-CEs / BAs
Congress – Healthcare Privacy Bills (cont’d)

- **Smartwatch Data Act (S. 2885, 116th) – Sens. Cassidy and Rosen**
  - All about consent: Prohibits the transfer, sale, sharing, or allowance of access to any consumer health information (unless aggregated or anonymized) to a domestic information broker or domestic entity
  - **Exceptions:**
    - “Informed consent”
      - Information is provided to a CE
  - Stricter requirements for the transfer of data to foreign entities
  - Enforced by HHS as if violation of HIPAA
- Covered organizations are state public health authorities as well as app developers
- Restricts processing and transfer of public health emergency contact tracing data (consent must be “prior affirmative express consent”)
  - Covers contact tracing data “linked or linkable” to individual or device
- No preemption
- Private right of action:
  - Violation of law is “injury in fact”
  - Up to $1,000 per violation for negligent
  - Up to $5,000 per violation for reckless, willful or intentional

- Covered entities do not include public health authorities; includes entities under FTC jurisdiction and common carriers & nonprofits
  - This means Senate Commerce maintains jurisdiction of the bill
- Restricts processing and transfer of covered data (consent must be “prior affirmative express consent” – less content to it than S. 3749)
  - Covered data does not include “de-identified” data (data not reasonably linked or linkable to individual)
- Preempts state laws dealing specifically with COVID-19 privacy (covered purposes)
- No private right of action, but enables state AGs to enforce
Exposure Notification Privacy Act (S. 3861, 116th) – Sens. Cantwell and Cassidy
- Covered entities do not include state public health authorities; they are “Operator of an automated exposure notification service” subject to FTC jurisdiction and non-profits and common carriers (universities, Verizon)
  • Senate Commerce maintains jurisdiction
- Restricts processing and transfer of data (no “commercial purpose”), consent must be “prior affirmative express consent” – more content than S. 3663
  • Covered data excludes de-identified data (not linked or reasonably linkable to an individual)
  • Federal agencies may not access data except for purposes under Act
- No preemption
- No private right of action, but enables state AGs to enforce
SAFE DATA Act (S. 4626, 116th) – Sen. Wicker, Thune, Blackburn, Fischer
- If compliant w/ HITECH, deemed in compliance w/ Act
- Prior, affirmative express consent for “sensitive personal information”
  - Includes “any covered data that describes or reveals the diagnosis or treatment of the past, present, or future physical health, mental health, or disability of an individual”
  - Opt-out for non-sensitive data
- Small business exemption – high threshold, only from some core components of bill
- Consumer rights:
  - Transparency (privacy policy disclosure); access; deletion, correction and portability
- Risk assessments
- Preemption
- No private right of action, but State AGs can enforce
COPRA (S. 2968, 116th) – Sens. Cantwell, Schatz, Markey, Klobuchar
- If compliant w/ HIPAA, deemed in compliance w/ Act, except Sec. 107 (the data security requirements)
- Prior, affirmative express consent for “sensitive personal information”
  - Broader definition than S. 4626, includes browsing history, email, phone number
    - Includes “any information that describes or reveals the past, present, or future physical health, mental health, disability, or diagnosis of an individual.”
  - Opt-out for non-sensitive data (FTC rulemaking)
- Small business exemption – low threshold, but exempt from entire bill
- Consumer rights:
  - Transparency (privacy policy disclosure); access; deletion, correction and portability
  - Risk assessments
  - No preemption
- Private right of action (injury in fact):
  - Up to $1,000 per violation per day, punitive damages, etc.
Congress – General Privacy (cont’d)

- Bipartisan House Energy and Commerce Committee Staff Draft
  - Relationship to HIPAA is undetermined (this sec. left blank)
  - Consent may be implied by context if “consistent with the reasonable consumer expectations within the context of the interaction between the covered entity and the individual”
  - Health information is part of “sensitive covered information” (the broader def’n uses the “linked or reasonably linkable” construct and “health information” is info that “relates to the physical or mental health or condition of an individual that . . . Was created, received or inferred by an online health product or service”, among other things)
  - Small business carve-out: Partial, however:
    - If annual revenue $25 mn or less, etc., can participate in an “approved compliance guideline” program, shielding participating companies from direct liability
  - Preemption and private right of action left blank (no agreement yet)
Summary

- **Current law:**
  - More data will flow out of HIPAA umbrella and into FTC jurisdiction
  - FTC will be working harder to enforce UDAP in healthcare data context

- **States are very active on privacy, including healthcare privacy outside HIPAA:**
  - California
  - Washington
    - Various states considering proposals that are variations of these
    - Massachusetts: considering a California law variant

- **Europe doesn’t silo healthcare privacy from “general” privacy**

- **Congress is active on privacy but bigger / other fish to fry:**
  - COVID-19 privacy bills
  - All of them are held up until there is resolution on:
    - Preemption
    - Private right of action