WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Key Developments in Health Data Protection and Cybersecurity

May 9, 2024

Kirk Nahra
Shannon Togawa Mercer

Speakers

Kirk Nahra

Partner
WilmerHale
@KirkJNahrawork
kirk.nahra@wilmerhale.com

Shannon Togawa Mercer

Counsel
WilmerHale
@togawamercer
shannon.mercer@wilmerhale.com

Agenda

- Current Landscape of Health Data Regulation
- What is health information or health data?
- Challenges in Health Information Protection
- HHS Enforcement and Settlements
- State Attorney General Enforcement
- Examples of HIPAA Enforcement by State AGs
- State Comprehensive Privacy Laws and Dobbs Laws
- Washington's My Health My Data Act
- The Federal Trade Commission
- Healthcare Data breaches

Current Landscape of Health Data Regulation

- HIPAA has historically been the primary discussion point for regulating health privacy in the United States
- Regulators and legislatures are increasingly paying attention to “non-HIPAA” health data or regulating HIPAA data in other ways
- Notable developments in recent years have included:
  - State comprehensive privacy laws
  - New consumer health privacy laws
  - “Specialty” laws related to Dobbs
  - Increased enforcement by the FTC and state AGs
  - Pixels/location data as health data
- These changes are:
  - Implicating more companies that previously did not have significant restrictions for the processing of their data
  - Bringing new regulators into the fold (outside of OCR)
  - Making the compliance environment more challenging for industry, not at all clear “privacy” is better

Current Landscape of Health Data Regulation

- **Observations from Practice:**
  - The “law” is changing constantly. Varying standards for different entities with the same information in different contexts. Many laws covering the same information
  - Increasing confusion about what constitutes “health information” or “health data” and why it should be protected
  - Aggressive enforcement without meaningful clear law
  - Real possibility that confusion and compliance will adversely impact the health care system

What is Health Information or Health Data?

- HIPAA applies to certain information held by certain people in certain situations (mainly doctors, hospitals, health insurers and their service providers). For this reason, it does not cover all health information
- The overall health care ecosystem has seen that there are all kinds of "health relevant data" - all kinds of personal data that isn't obviously about your health (income, marital status, television habits, shopping patterns, voting) have implications for health care issues
- What is "outside" of HIPAA is growing. For example, web sites gather and distribute healthcare information without the involvement of a covered entity (from commercial web sites (e.g., Web MD) to patient support groups to the growth of personal health records to mobile apps and wearables)

What is Health Information or Health Data?

- **Examples of the breadth of health information:**
  - HIV/Mental Health/Substance Abuse Information
  - Your name and address as a patient
  - Foot surgery records (even for this compare my tennis injury to Lebron James seeking a new contract after a major injury)
  - Search history of medical information
  - Location data
  - Voting Records/Purchasing Habits/Television Watching (used to evaluate medical issues)
  - Address as a patient
- **Raising questions about why we are protecting this information in this way**

Challenges in Health Information Protection

- Emerging rules/practices for artificial intelligence (note the FTC chair statements on using health data for AI)
- FTC statements about not using health data to train AI models
- Lots of questions about data use
- Expect challenges to de-identification practices
- Increasing complexity about using data from in and out of HIPAA
- Some history of OCR being helpful and reasonable

HHS Enforcement and Settlements

- Cases still fit into particular patterns
- Mainly access cases in recent years
- Handful of security breach cases (including recent resolution of an investigation that began in 2015)
- Small number of "send a message" cases (e.g., media contacts)
- Investigations are more thorough and more burdensome and more time consuming
- Increasing pressure to do more on both audits and investigations
- Fairly small number of penalty actions
- Still generally reasonable (some question about this statement as a continuing matter)
- Continuing impact of MD Anderson case

State Attorney General Enforcement

- **Authority comes from:**
  - HIPAA (and "mini" HIPAA rules)
    - HITECH Act amended HIPAA and gave state AGs the authority to bring civil actions on behalf of state residents who have been impacted by HIPAA violations
  - State breach notification laws/data security laws
  - State unfair or deceptive acts or practices laws
  - State comprehensive privacy laws
  - State consumer health data laws
  - Other laws that create specific processing obligations for specific categories of data, e.g.:
    - Biometric privacy laws (e.g., in Illinois, Texas, and Washington)
    - Genetic privacy laws (e.g., in CA and UT)
    - IoT device laws (e.g., in CA and OR)
    - Older state laws relating to sensitive conditions (e.g., HIV status or mental health history)

State Attorney General Enforcement

- In cases where state AGs bring enforcement decisions, OCR may bring its own separate claims (and vice versa)
- Limited enforcement early on by state AGs but has picked up in recent years
  - Most cases involve data breaches and violations of the HIPAA Security Rule (in addition to violations of state-specific consumer protection or data security laws)

State Comprehensive Privacy Laws and Dobbs Laws

- **At least sixteen states have passed some form of "comprehensive" privacy law *(Maryland will make 17 once signed by the governor)*:**
  - This does not include Florida, which has passed a privacy law that applies to specific types of companies (though it does create some compliance obligations for entities that process sensitive data)
- These are laws of general applicability–instead of regulating specific types of data or data processing activities, these laws create overall data processing obligations for entities that they apply to
  - However, all of these laws exempt data that is processed pursuant to HIPAA and many create entity wide exemptions for covered entities and business associates regulated under the law
- There are many similarities between these laws but also meaningful differences

State Comprehensive Privacy Laws and Dobbs Laws

- **Specific state laws being passed to protect Dobbs related data**
  - Creating enormous compliance challenges both in and out of HIPAA
  - Very hard to reconcile with HIPAA provisions
  - Threatens broader health care issues (connect with what was not proposed in HIPAA changes)
  - Is the goal of protecting this data going to create other problems?

Washington's My Health My Data Act

- The MHMDA represents a major new category of privacy law—one focused exclusively on "consumer health data"
- Passed very quickly, at least partly in response to the Dobbs decision
- Broad reach beyond traditional healthcare entities
- Major attack on health-related advertising
- Lots of ambiguities—that will be played out in court because of private right of action
- Already inspired copycats (in Nevada and Connecticut), with more likely to follow—big issue is if other states are going to also include a private right of action

- **What makes MHMDA different?**
  - Extremely broad in its scope:
    - Regulates "consumer health data," which is defined extremely broadly, including categories of information such as:
      - Individual health conditions, treatment, diseases or diagnoses
      - Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies
      - Data that identifies a consumer seeking healthcare services
      - Any information that a regulated entity processes to associate or identify a consumer with [other categories of consumer health data] that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred or emergent data by any means, including algorithms or machine learning)

The Federal Trade Commission

- Emerging as a leader in health privacy enforcement
- Broad definition of health data – anything that conveys information – or enables an inference about a consumer's health
- Broad interpretation of unfairness authority to curb allegedly harmful practices
- Multiple policy statements over the past year around health data, as well as active rulemaking
- Continued focus on substantive limitations and remedies that raise reputational/business issues for companies

The Federal Trade Commission

- A number of important cases – breaking new ground on use of health data issues (and data that doesn't really seem like health data but can be in some situations – e.g., location data)
- They are trying to change behavior without new law or regulations
- They are also changing regulations – after guidance and after enforcement cases
- Using a law on health data breaches to define appropriate behavior for overall use/disclosure of health information

The Federal Trade Commission

- FTC is aggressively pursuing the use of tracking technologies that collect personal health data
- Through *GoodRx* and *BetterHelp*, FTC has established that the failure to obtain affirmative express consent from consumers before transferring health information to third parties for advertising purposes and the third parties' own purposes (e.g., developing their own products) is an unfair business practice
- Remedies include permanent ban from disclosing consumer health information to advertisers, directing third parties to delete data
- Companies need to understand tracking technologies on their websites, how they work, and what contractual arrangements are in place (easier said than done)

The Federal Trade Commission

- Policy Statement on Biometric information and Section 5
  - "Using biometric information to identify consumers in certain locations could reveal sensitive personal information about them—for example, that they have accessed particular types of healthcare"
  - Expansive view of "biometric information"
  - Provides overview of factors supporting an unfairness determination
- *FTC v. Rite Aid*
  - *Rite Aid* allegedly failed to take reasonable measures to prevent harm to consumers from its use of facial recognition technology and violated a 2010 FTC order relating to data security and vendor management
  - *Rite Aid* is prohibited from using facial recognition for five years; data and model deletion; consumer notice and redress; data retention

Healthcare Data Breaches

- Increasing array of incidents involving multiple layers and many branches
- Meaningful practical challenges for every entity in the layers and branches
- Some history of OCR being helpful and reasonable

Takeaways

- Many moving parts on overall regulation of health care privacy
- Growing questions about what “health data” is and why/how it should be treated differently from other data
  - Regulators are beginning to think about “data issues” together—not just privacy, data security, artificial intelligence, competition, consumer protection, etc. as separate areas of focus
- State law creating more complications
- Federal debate not likely to “solve” these problems
- Real questions about whether the rules for privacy will get in the way of a working health care system – and what the implications of that will be for consumers

Takeaways

- Difficult to build a compliance approach due to divergence in legal requirements across jurisdictions and data types
- Anticipate meaningful test cases from regulators and investigations that are designed primarily to gather information about ongoing practices
- Increasing number and scale of breaches
- Investigations are complex, often starting at one place and ending somewhere else entirely

Questions & Contacts

Kirk Nahra
Partner
WilmerHale
@KirkJNahrawork
kirk.nahra@wilmerhale.com

Shannon Togawa Mercer
Counsel
WilmerHale
@togawamercer
shannon.mercer@wilmerhale.com

Additional reading

- **FTC Emerges as Leader in Health Privacy Enforcement:** https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230804-ftc-emerges-as-leader-in-health-privacy-enforcement
- **HHS OCR Settles with iHealth Solutions Over Alleged HIPAA Violations:** https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230720-hhs-ocr-settles-with-ihealth-solutions-over-alleged-hipaa-violations
- **Washington AG's Office Releases New Guidance for the My Health My Data Act:** https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230713-washington-ags-office-releases-new-guidance-for-the-my-health-my-data-act