Managing Long Term Risks for Privacy, Cybersecurity and AI

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

Kirk J. Nahra
WilmerHale
202-663-6128
Kirk.Nahra@wilmerhale.com
@kirkjnahrawork

Robyn Eckerling
Tempus
robyn.eckerling@tempus.com

Today's Discussion

- Health care privacy was one of the driving forces of US privacy law – still a key source of learning on privacy issues
- Starts from the idea that health care information is "different" from other information and deserves "more" protection
- The law used to be reasonably simple – but now is anything but.

Today's Discussion

- And now we have lots of conflicts and confusion and contradictions
- The result being growing chaos and an overall mess – and a growing likelihood that the "law" in this area - designed to protect health privacy – actually will get in the way of a working health care system and won't help patients

Today's Discussion

- The bad news is that this chaos is growing and shows no signs of slowing
- Realistic concerns that "privacy" law is getting in the way other aspects of heath care policy
- The good news is . . . . . TBD (if any)

Today's Discussion

- We have a few goals for today.
- We want to explain why the law of health care privacy is a growing mess
- We want to discuss some of the enforcement implications for this development
- We want to discuss operational steps within your companies and clients
- And then give you some specific advice on how best to navigate this area and think about specific risks

Why do we say this?

- 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 “health information” means – and why it should be protected (more than other data)
- Aggressive enforcement without meaningful clear law
- Increasing confusion, complications and inconsistencies

Health Care Privacy Framework

- HIPAA at the forefront
- State "HIPAA-Like" Laws (e.g. CA CMIA, TX)
- State Overall Privacy Laws (some with specific heath challenges - e.g., Maryland)
- State laws on sensitive conditions
- "Non-HIPAA" health data – Washington "My Health My Data" law (Now New York and likely more)
- Medical Research principles (US and global)
- Other federal laws (Part 2 substance abuse rules, ADA, etc)
- International principles and standards

So what are we even talking about with Health Privacy?

- Is it about the information?
- What is health information?
- Does it deserve “more” protection and if so why?
- Hint – It is getting harder and harder to explain why everything we are thinking of as health information deserves extra protection

Health Information

Is there something "different" about it?

1. HIV/Mental Health/Substance Abuse Information
2. Your name and address as a patient (protected by HIPAA)
3. Foot surgery records (even for this compare my tennis injury to Lebron James seeking a new contract after a major injury)
4. Search history of medical information
5. Location data
6. Voting Records/Purchasing Habits/Television Watching (used to evaluate medical issues)

Health Information

- Growing breadth about what "the law" treats as health information
- Growing breadth about what we think of as health information or what data can be used/useful as health information (both in real health care and in marketing)
- All of this makes a rationale for treating health data as "sensitive" much harder

Confusion

- So is health privacy about “the health care industry”?
- HIPAA defines “covered entities” - based on portability of health insurance coverage and standard electronic transactions
- Was never an overall health privacy law
- More and more health care activity beyond these categories (e.g., non-health insurance lines, pharma, consumer health, wearables, mobile apps, patient support groups, personal health records)
- Social determinants of health creating more confusion

The New Law

Consumer Health Law

- Consumer Health Laws (e.g., Washington My Health My Data Act) – Driven by Dobbs but applies much more broadly
- Much broader range of data and entities than anyone would normally think of as “health” – data that can lead to “inferences” about health (with no clear limiting principle)
- Impacting wide range of entities who aren’t “health” companies
- Impacting clinical trials and finding patients
- Sometimes bizarre implications on “location” data

Dobbs Laws

- Specific state laws being passed to protect Dobbs related data
- California law that protects reproductive rights data - which then seems to require "segregation" of this information from other parts of the medical record
- Also state AGs trying to force "more" disclosure of this information (while others pushing for "less" disclosure)
- **Is the goal of protecting this data going to create other problems?**

"Other" Law Issues

- Impact of state "comprehensive" privacy laws (which *generally* exempt HIPAA) (**be smart about relying on these exemptions**)
- The lessons of the Part 2 Substance Abuse Rules
- Potential implications of the new rule - coming soon – on opioids and social service organization issues
- What about things like trackers?

How is your health information protected under CCPA?

1. HIPAA protected information (generally exempted from CCPA)
2. CMIA covered companies/information (generally exempted from CCPA)
3. Common Rule/Clinical research (generally exempted from CCPA)
4. CCPA – probably covers your health information if it isn't exempted
5. BUT CCPA doesn't cover non-profits
6. And CCPA didn't generally cover employers and employee information (note that it does post 7/1/2023) (other states don't)

The results of all of this are:

- No realistic basis for consumers to understand the rules for their data
- Harder and harder for businesses to understand the rules (including whether any “rules” are applicable to them)
- This complexity can result in more expensive health care, less reliable health care, difficulties with medical research, challenges to building useful AI, difficulty with investments
- Who is this good for?

Conclusions

- We have lost the narrative on health care privacy
- Growing questions about what “health data” is and why/how it should be treated differently from other data
- State law creating more complications
- Federal debate not likely “solve” these problems
- Just too much law at this point without a coherent overall approach
- 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

Key Learning from Recent Enforcement

Long Tail Considerations

- What do we mean?
- Areas where you may be “ok” today because of enforcement priorities - but there may still be issues with your decisions today in the (not too far off) future

False Claims Act – Cyber

- Relatively recent initiative of DOJ
- Also important whistleblower risks
- Has crossed Administrations at this point
- Meaningful look-back periods
- Can be tied to a specific incident or some other "prompt" – including internal understandings of CISO or others

Some Examples (False Claims Act)

- Illumina Inc. (2025) has agreed to pay $9.8 million to resolve allegations that it violated the False Claims Act when it sold to federal agencies certain genomic sequencing systems with cybersecurity vulnerabilities.
- The settlement resolves allegations that, between February 2016 and September 2023, Illumina sold government agencies genomic sequencing systems with software that had cybersecurity vulnerabilities, without having an adequate security program and sufficient quality systems to identify and address those vulnerabilities.

Some Examples (False Claims Act)

- Health Net Federal Services and its corporate parent Centene Corporation have agreed to pay $11,253,400 (2025) to resolve claims that HNFS falsely certified compliance with cybersecurity requirements in a contract with the DoD to administer the TRICARE health benefits program for servicemembers and their families.
- The settlement resolves allegations that, between 2015 and 2018, HNFS failed to meet certain cybersecurity controls and falsely certified compliance with them in annual reports to DHA that were required under its contract to administer TRICARE.

False Claims Act

- Repeated cases where cyber statements go back 8-10 years or more
- Can be triggered by a specific event or by many other developments
- Ongoing incentives for whistleblowers
- **Tip** – Pay close attention to internal concerns about security controls
- **Tip** - Don't make certifications pro forma – do real ongoing evaluations

AI is Long Term Also

AI Development 2025-2026

- Federal policy has shifted from "precautionary restriction" to "accelerated dominance."
- Executive Order 14179
  - Deregulation Focus: Revocation of previous "burdensome" AI requirements (EO 14110) to clear path for private sector innovation.
  - National Preemption: DOJ AI Litigation Task Force (est. Jan 2026) actively challenging "onerous" state-level AI laws to ensure a unified national market.
- Innovation over Compliance
  - Regulatory Relief: Introduction of "AI Sandboxes" in health tech to allow experimental model training with reduced liability.
  - Global Leadership: Prioritizing hardware, chips, and energy-efficient health AI as matters of national security.

HHS Artificial Intelligence (AI) Strategy Overview

- Pillar 1: Governance & Trust: Institutionalize transparent risk management and oversight, with stringent controls for "high-impact" AI applications affecting health outcomes.
- Pillar 2: Unified Infrastructure: Develop an "AI-integrated Commons" providing shared computing power, secure data repositories, and reusable models across the Department.
- Pillar 3: Workforce Empowerment: Equip employees with secure AI assistants ("copilots") and role-based training to reduce administrative burdens and increase productivity.
- Pillar 4: Gold-Standard Science: Embed scientific rigor, reproducibility, and open-data principles into AI-augmented research and regulatory approval processes.
- Pillar 5: Health Delivery Modernization: Deploy AI tools for clinical decision support and risk stratification to improve individual patient and population health outcomes.
- Agile Acquisition: Implement modular contracting and "Tech Sprints" to attract innovative vendors and avoid vendor lock-in.

Enforcement Trends

- “AI-Washing”
  - FTC enforcement in 2026 (e.g., Growth Cave) has moved toward truth-in-marketing.
    - Prohibited Claims: Barring claims that AI "automates 100%" or "maximizes profits" without specific substantiation.
    - Algorithmic Disgorgement: Still the "nuclear option" for models trained on non-consensual health data.
- Risk Management
  - NIST RMF 2026: Move from "Ethics" to "Assurance." Focus on measurable performance metrics.
  - Trustworthy Infrastructure: New NIST Profile (April 2026) for AI in Critical Health Infrastructure.
  - Transparency Mandates: Requirement to notify users when interacting with clinical chatbots (now law in 36+ states as of Q1 2026).

Disgorgement

- FTC has brought a series of cases where disgorgement of models has been a remedy
- A major impact on companies – clearly changes the risk management profile
- This is a real sanction - with real long tail implications

Disgorgement – Going Forward

- Be thoughtful about your decisions today (even if no one is currently watching)
- Be cognizant of any existing FTC (or other) agreements (even tangentially related) that can be used for future enforcement (with dollars)
- Be cognizant of how the FTC builds its "unfairness" jurisdiction
- Be thoughtful about permissions (both from consumers and commercial customers)

Privacy Can Have Criminal Implications

Some Examples – HIPAA Criminal

- A federal grand jury in Pennsylvania has indicted a former patient coordinator on several counts of wrongfully obtaining and disclosing the health information of others.
- Five former Methodist Hospital Employees and one outsider have pled guilty to unlawfully disclosing patient information in violation of HIPAA. The outsider paid the employees to provide him with names and phone numbers of Methodist patients who had been involved in motor vehicle accidents. After obtaining the information, the outsider sold the information to third persons including personal injury attorneys and chiropractors.

Some Examples

- A former physician with medical practices admitted wrongfully disclosing patients' protected personal health information.
- Pleaded guilty to conspiring to wrongfully disclose patients' PHI to pharmaceutical sales representative

Some Examples

- U.S. District Court judges sentenced three former district managers of a pharmaceutical firm to a series of criminal HIPAA violations that have been linked to healthcare fraud.
- The three perpetrators committed criminal HIPAA violations by illegally accessing patients' PHI in order to drive sales of specific drugs

Criminal Issues

- DOJ Data Transfer Rules
- Expectation of meaningful enforcement – perhaps across administrations
- Concerns today, long term concerns with events tomorrow
- Where potential criminal issues arise (e.g., a fraud claim) – be aware of how data issues can underlie the claims

De-Identification

- Evolving standards under existing and new law
- Growing technology concerns about re-identification risks
- Standards typically tied to current knowledge – but what happens “later” if there is re-identification?
- May not be a violation of de-id provisions – but is there some other kind of “problem”
- Be thoughtful about existing standards, real evaluations of risk, additional contract requirements, etc. (including DOJ rules where de-id data not exempt)

Key Considerations for Risk Management

Key Considerations

Security policies and incident response preparation

- Stay on top of technological developments, understand how most incidents occur, and evaluate the impact of regulatory enforcement actions on your business
- Note where you do not have multifactor authentication in place, as well as every place in your company that you store or collect Social Security numbers or other sensitive personal data

Data minimization *vs.* maximization

- Data protection laws generally require entities to engage in data minimization as a best practice
- This runs contrary to the practices that most companies have engaged in for years—*collect as much data as possible and figure it out later*

Mind the Gaps

Data Map

- Important to understand what data is collected and for what purposes in order to properly assess compliance risk
- Employee and commercial data also fall into scope of certain laws and in certain contexts

Sensitive Data

- Regulators have especially focused on bringing enforcement actions that involve “sensitive” data categories
- Pay special attention to obligations tied to the processing of health data, children’s data, genetic data, etc.

Litigation Risk

- Certain data practices (such as the use of third-party pixels and biometric identifiers) create unique risks due to certain laws that create private rights of action

Mind the Overlaps

M&A integration

— Large-scale security breaches tend to involve situations where a recently acquired company is attacked before its security practices are integrated with the parent company

Business expansion

— A small, acquired company may not be subject to many of the US state laws

— Once acquired, however, a purchaser will inherit a set of practices that may not have violated law before the acquisition—but now will

Artificial Intelligence

— Companies should evaluate their approach to AI alongside privacy law

Operational Considerations - AI

The 4-Phase Implementation Roadmap

- Initiation: Appoint Governance Committees and define "Responsible AI" principles.
- Impact Assessment: Conduct mandatory DPIAs and bias audits for clinical tools.
- Framework Rollout: Establish Acceptable Use Policies and Human-in-the-Loop (HITL) requirements.
- Continuous Monitoring: Drift detection and safety reporting.

HHS "Total Product Lifecycle" Mandate (2026)

- Shifts oversight from a one-time pre-purchase audit to a persistent monitoring model.
- "Total Product Lifecycle" (TPLC) oversight for health-related AI devices.
- Mandates ongoing verification of model safety, efficacy, and data integrity post-deployment.

Operational Considerations - AI

Transition: From Ethics to Technical Assurance

- Governance teams evolving from "Ethics Boards" to technical "Assurance Committees."
- Primary focus on Measurable Performance Indicators (MPIs) rather than broad ethical statements.
- Prioritizes technical security vulnerabilities, specifically protection against model-injection attacks.

Multi-Disciplinary Governance Structure

- CISO & Security: Oversight of AI supply chain risk, SBOMs, and technical vulnerabilities.
- Clinical Leadership: Validation of medical accuracy, algorithmic bias, and patient safety.
- Legal & Privacy: Managing HIPAA compliance and navigating federal/state preemption.
- Data Science: Technical performance monitoring and managing "performance drift."

Predictions and Conclusions

Predictions

- Federal privacy push—success seems unlikely
- Unlikely that there will be no new state privacy laws again
- States are likely to continue filling any real or perceived federal regulatory/enforcement gap
- AI will continue to draw regulatory attention
- DOJ DSP enforcement
- Anticipate meaningful test cases from regulators and investigations that are designed primarily to gather information about ongoing practices

Key Considerations

- Specific areas of concern
- Pixels/trackers
- Marketing (to both consumers and professionals)
- Overall consent issues
- Data Security
- Location issues
- Involvement with data brokers

Key Considerations

- Be thoughtful about relying on a no enforcement" approach from any administration guides legal advice and relevant decision making
- Be cognizant of uses of sensitive data
- Be conscious of bias and discrimination generally - to understand where there are potential gaps and how to think about them
- Be thoughtful about the sources of your data
- Make sure you are fixing identified meaningful security problems

Questions?

Kirk J. Nahra
WilmerHale
(202) 663-6128
Kirk.Nahra@wilmerhale.com
@kirkjnahrawork

Robyn Eckerling
Tempus
robyn.eckerling@tempus.com