Navigating Privacy in the Life Sciences Industry

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

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

Kimberly S. Gray
Global Chief Privacy Officer
IQVIA
Kim.Gray@iqvia.com

Today's Discussion

- Some of the hot topics in health privacy today for the life sciences industry
- Overall developments impacting enforcement, policy, the overall health care system, investment in health care businesses and future legislation
- Lots of moving parts in an increasingly complicated environment
- Growing areas of tension between different policy goals

Today's Discussion

- Key legal issues for today
- Then discuss practical operational issues – what are your major challenges in dealing with this increasingly challenging legal environment

A sub-title for the presentation

Health care privacy is a growing mess

Why do I 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

Setting the stage

- Pharma industry generally not subject to HIPAA
- Many learned privacy through GDPR
- Now, as they gather more information from more places, must navigate increasingly complicated state laws and various intersections with HIPAA
- So – unlike HIPAA entities – no “core” framework to guide legal decisions

Setting the Stage

- Life Sciences – drug/product development overall creates meaningful complexity
- Balancing HIPAA with research with state law with international principles – where rules change depending on specific roles and stage in the broad business process
- Risk profiles change as business model evolves

Health Care Privacy Framework

- HIPAA at the forefront (but mostly not for life sciences)
- State “HIPAA-Like” Laws (e.g. CA, TX)
- State Overall Privacy Laws (e.g., CA, Colo, VA)
- “Non-HIPAA” health data – Washington “My Health My Data” law
- 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 entities? (HIPAA is very much driven by “who” has the information)
- Is it about the information?
- What is health information?
- Does it deserve “more” protection and if so, why?
- Should all “health information” be treated the same?

Health Information

Is there something "different" about it?

1. HIV/Mental Health/Substance Abuse Information
2. Your name and address as a patient
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

- HIPAA mostly treats all PHI the same
- Some modest changes, both more and less
- State laws increasing drawing lines
- How does this work? Who gets to decide? Does this work for health care overall?

Some key legal challenges today

State "comprehensive" privacy law

- Increasing challenges for health information and/or sensitive information
- New rules about consent, particularly for sensitive data
- Little "nuance" to make health care system work well

Washington – My Health My Data

- Consumer Health Laws – Driven by Dobbs but applies much more broadly
- Explicitly does not apply to HIPAA companies – but expect to have these issues pushed even for HIPAA covered entities
- Much broader range of data and entities than anyone would normally think of as “health” – data that can lead to “inferences” about health
- Key challenge with clinical trials and finding patients
- Spreading to other states (with different challenges)

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?

Overall Data challenges

- Emerging rules/practices for artificial intelligence
- 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

Multi Layer Breaches

- Increasing array of incidents involving multiple layers and many branches
- Meaningful practical challenges for every entity in the layers and branches
- Creates enormous regulatory and business risk

New Administration/OCR

- Dobbs Issues – the New Rule (would be pulled, certainly won't be enforced)
- Gender Affirming Care (impact if any)
- Civil Rights for physicians
- Civil rights investigations of health care facilities for DEI activity (at least a resource issue)
- No real clue yet on actual OCR enforcement of HIPAA privacy and security rules

New Administration/OCR

- Now moved to a different structure within HHS
- An overall effort to focus on “waste, fraud and abuse” – (not particularly privacy things)
- HIPAA Security Rule NPRM – likely pulled
- Curious issue of opioid rule with social service organization disclosures

The FTC Moving Forward

- The New Chair - In his "application" - that under his stewardship the agency would "stop abusing FTC enforcement authorities as a substitute for comprehensive privacy legislation."
- There will be "No more novel and legally dubious consumer protection cases."

More Insight

- In his first week as Chair, he announced that the incoming Republican majority at the FTC "will end the previous administration's assault on the American way of life, and we will usher in a new Golden Age for American businesses, workers, and consumers."

Going Forward

- The “commercial surveillance” rulemaking is dead
- While “deception” cases will continue, likely much less use of “unfairness” authority.
- “The majority has developed a penchant for pressing aggressive and novel theories in complaints it knows will not be litigated and relying on those unadjudicated complaints as a form of precedent for subsequent Commission action.”

Going Forward

- FTC Act "does not limit how someone who lawfully acquired those data might choose to analyze those data.
- The HBNR may go down (at least will be used less) – dissented from final rule saying the rule "exceeds the bounds Congress clearly established" and revised definitions are not "consistent with the statute."

Going Forward

- Continued deception cases
- Continued cyber breach cases
- Likely attention to children's data (although rules may change again)
- Likely review of content moderation (not quite privacy)

The Counter-punch - State AGs

- Likely continued focus on cyber incidents (both red and blue AGs)
- Likely increase in “privacy” enforcement from blue states
- Continued passage of new state laws (comprehensive laws, consumer health, Dobbs, other consumer issues, maybe AI)

State AGs and Health Care

- Lots of interest in health care issues and health data generally
- We can expect them to pick up some of the slack from the federal government
- We can expect them to continue with security enforcement generally (and not a red state/blue state issue)
- They often don't seem to know or necessarily care about the lines in the rules (e.g., data breach laws that exempt HIPAA)

How to Look Forward

- Cybersecurity remains enormously important (both because of enforcement and other problems)
- Take a longer view in advising clients (no enforcement now doesn't mean its legal)
- AI Perspective
- Be thoughtful about uses of sensitive data in any context

A national privacy law

- Not likely to make things "better" for health care industry
- Core health care not part of the debate – leaving big gaps in overall strategic thinking
- Likely to just add another layer of complexity (especially if no full preemption)

Operational Challenges

- Navigating across the country with different laws
- Navigating around the world
- Creating a program for “marketing” in general
- Developing appropriate research efforts
- De-Identification issues
- AI complexities

Conclusions

- Lots of 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
- State law creating more complications
- Federal debate not likely “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

*Top 5 life sciences privacy concerns from a practical point of view – *May 2025 edition (and purely subjective)*

- Administrative activities, state laws/regs
- Privacy-adjacent laws and regulations
- Third party Risk Mgt
- The “B” word
- Data Subject Requests

Administrative Activities, State Laws/Regs

Executive Orders

- Bulk Transfers

Department of Health & Human Services initiatives

- Autism
- Vaccines
- Pandemic

Sanctioned countries

Trial recruitment

Privacy-Adjacent Laws, Regulations—and expectations

- Artificial intelligence
- Cybersecurity
- Information governance
- Web trackers, cookies
- Marketing
- TCPA
- CAN SPAM

Third-Party Risk Management

Vendors

- Vendor approval
- Ongoing oversight
- Lack of choices in vendors
- Incidents

Sites

- Oopsies!
- Oversight
- Targets for breaches
- Overall risk posture

The "B" word (data breaches)

Security incidents

- The reason (targets)
- The team
- The data
- The processor or controller
- The scorecard
- The regulator(s)
- The notifications
- The after-action review, the CAPAs, the Audits

Data Subject Requests

Wishing we had all seen the writing on the wall, eh? (the 3rd party cottage industry)

- Started in EU and fizzled
- Alive and well in US

Daniel's Law versus others

Teaching colleagues about the differences in requests

- Please quit saying "opt out" for everything
  - Do not share, do not sell, deletion (or maybe even an opt-out)

Questions?

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

Kimberly S. Gray
Global Chief Privacy Officer
IQVIA
Kim.Gray@iqvia.com