WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Why Health Care Privacy is a Mess

Kirk J. Nahra
WilmerHale
Washington, D.C.
202.663.6128
Kirk.Nahra@wilmerhale.com
@kirkjnahrawork

Today's Discussion

- An enormous amount of change in the health care privacy legal structure in recent years – with more to come
- These developments are impacting enforcement, policy, the overall health care system and future legislation
- Lots of moving parts in an increasingly complicated environment – with increasing possibilities of disruption to health care
- Very challenging to see how this "mess" is improving privacy and security, for consumers or the industry
- Answer your questions

Why do we say health privacy is a mess?

- 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
- Raising the stakes substantially for investment in new ideas about health care

Confusion – The Health Care Industry

- What is the health care industry?
- HIPAA defines “covered entities” - based on portability of health insurance coverage and standard electronic transactions
- Does this make sense anymore?
- More and more health care activity beyond these categories
- Still have health care providers who don’t have to follow the HIPAA Rules
- Social determinants of health creating more confusion

Confusion – Health Care Information

- What is health information?
- Does it extend to “health relevant” information – doesn’t look like health information but used in health decision-making or to make assumptions about an individual’s health
- Does it deserve “more” protection and if so, why?

Health Information

- Is there something “different” about it?
  - 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)

Pixels

- Unexpected situation
- Guidance from OCR – clearly wrong in the beginning
- Revised guidance creates complete unmanageable lines
- Is a “click” health information?
- What is the point of consumer notice?

Consent (HIPAA)

- Purpose is to balance appropriate privacy protections with efficient and effective operation of the health care system
- An implicit recognition that “better” privacy protection would be bad for the health care system (and for its patients)
- Are recent developments incorporating this balance?
- Are there lessons to be learned for the broader debate on a national privacy law?

Consent

- Growing evidence that consent beyond HIPAA doesn't work well to protect individual privacy
- How is this approach of new activity going to work:
- Under the state laws?
- Under the FTC's guidance?
- In connection with AI training?
- In Dobbs situations?
- Is there enough thought about implications?

Pending Rulemaking/Policy Issues

- Social Service Organizations/Opioid Issues
- Pending rulemaking
- Additional disclosures to support social goals (food banks, religious organizations) balanced against patient interests
- Similar issues with disclosures to family members/caregivers in opioid addiction situations
- Privacy interests vs. other goals

Rulemaking/Dobbs

- Administration made a conscious choice to limit the scope of the rule changes
- Primary focus is on making it harder for law enforcement to access certain reproductive rights information
- Did not revise consent approach for Dobbs information/A wise choice
- Likely future litigation involving law enforcement

Confusion/Complexity

- Other regulators – the FTC
- Chair Khan and staff Leadership setting out an agenda
- They aren't shy about pushing their agenda
- Very explicit about its intentions
- Essentially saying "we missed our chance to do better on the Internet generally and are not going to miss our chance again"
- Query whether the FTC – today – is more important than OCR in regulating health privacy

The FTC and Health Care

- Clearly pushing the envelope as far as they can (and arguably further than statutory authority permits in the health breach notification rule)
  - For example, change to definition of “personal health record” notwithstanding clear definition in the HITECH authorizing statute
- Looking at more aggressive remedies (particularly data disgorgement)
- They assert authority over HIPAA entities (although they don’t use it much)
- Expect potential cases at the margins – AI, health advertising online.
- Remember and learn from their history on data security - will there be pushback?

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

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?

Maryland Comprehensive Privacy Law

- Maryland Online Data Privacy Act of 2024 - one of the most recent “comprehensive” state privacy laws
- Consumer health data - Defined as “personal data that a controller uses to identify a consumer’s physical or mental health status.” Defined also as “sensitive data.”
- MODPA distinctively prohibits the sale of sensitive data and restricts any collection, processing, or sharing of such data, unless it is "strictly necessary" to deliver or maintain a product or service specifically requested by the consumer. This comprehensive ban on the sale of sensitive data is unprecedented among state privacy laws, which either use a notice-and-consent or opt-out framework.

How is your health information protected under CCPA?

- HIPAA protected information (generally exempted from CCPA)
- CMIA covered companies/information (generally exempted from CCPA)
- Common Rule/Clinical research (generally exempted from CCPA)
- CCPA – probably covers your health information if it isn't exempted
- BUT CCPA doesn't cover non-profits
- And CCPA doesn't generally cover employers and employee information (changed somewhat under CPRA)
- How can consumers, businesses and others deal with this?

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

Health Care Privacy Framework

- HIPAA at the forefront
- State “HIPAA-Like” Laws (e.g. CA, TX)
- State Overall Privacy Laws (e.g., CA, Colo, VA)
- State laws on sensitive conditions
- “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

AI Development

- Chair Khan - Sensitive personal data related to health, location or web browsing history should be “off limits” for training artificial intelligence models. (WHY?)
- The FTC is working to create “bright lines on the rules of development, use and management of AI inputs.” Khan said.
- “On the consumer protection side, that means making sure that some data — particularly peoples’ sensitive health data, geolocation data and browsing data — is simply off limits for model training.”
- Khan said that companies that want to use data they’ve already collected for AI training also must actively notify users of the change.

Health Care and AI

- So the health care industry essentially can’t use its entire history to develop AI?
- Is that a position that says no AI in health care?
- Who is that good for?

The Future: What is the Right Approach

- Should there be an “overall” approach to health privacy, or something tailored to more specific situations?
- Compare California Consumer Privacy Act approach (general – although with lots of exceptions) – to something like a facial recognition law and to GDPR in Europe
- Rationale for much of health care privacy involves lots of stakeholders – well beyond many “other” aspects of privacy law
- Is there anything “different” about health information?
- HIPAA rules have careful nuance to make the (traditional) health care system work well

A different approach

- GDPR – Broad principles establishing data privacy and security law across the EU
- Protects all personal information in all settings
- Application to a wide range of US companies
- Health care industry simply part of the overall legislation
- Health care data considered sensitive information with certain special restrictions – no health nuance
- Not a recommendation but an alternative model

Health Care in the National Privacy Debate

- Lots of complicated issues – and not enough current thinking focused on these issues
- Health care industry is largely absent from the debate
- Others who are involved in the broader debate aren't thinking about this issue
- A key consideration involving the exemptions going forward
- The health care industry needs a position if the exemptions do not continue
- Does the health care industry want this fragmented field going forward?

The Newest Federal Proposal

- Paragraph (1) (GENERAL PREEMPTION) shall not be construed to preempt, displace, or supplant the following State laws, rules, regulations, or requirements:
  - (N) Provisions of laws that protect the privacy of health information, healthcare information, medical information, medical records, HIV status, or HIV testing.
- IN GENERAL.—A covered entity or service provider that is required to comply with the laws and regulations described in subparagraph (B) and is in compliance with the data privacy requirements of such laws and regulations shall be deemed to be in compliance with the related provisions of this Act (except with respect to section 9), solely and exclusively with respect to any data subject to the requirements of such laws and regulations.

The Newest Federal Proposal

— For purposes of subparagraph (A), the laws and regulations described in this subparagraph are the following:

(ii) Part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.)

(iii) Subtitle D of the Health Information Technology for Economic and Clinical Health Act

(iv) The regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996.

(See separate similar language on security)

Clinical Trials/Medical Research

- Known concerns about data sets being used for both overall research and development of AI
- Broad interest in expanding diversity of clinical trial participants
- Enormous (potential) benefits from research for “personalized medicine”
- Growing tension among health policy goals and privacy limitations
- Noticeable impact on ability to identify diverse audiences for clinical trials
- Concern about “permissions” for AI making AI data sets “worse”

De-Identification

- HIPAA standard remains the gold standard of de-identification
- While there are lots of questions, no meaningful examples of properly de-identified HIPAA data sets being re-identified
- Growing concern that there are not enough “experts” for de-identification
- Growing concern that the “non-HIPAA” health data will have an impact on re-identification possibilities
- Will Ai make this risk even worse?

Information Blocking Confusion

- High risk new regulations - subject to high potential enforcement
- General confusion
- Somewhat turns privacy/HIPAA on its head – some view as “if you are permitted you must do it.”
- Watch for ongoing abuses of the “opportunities” created by these rules

Overall Implications

- Customer confusion
- Overall complexity means higher cost and less reliability
- Increasing reluctance to share in some situations
- Will this have meaningful impact on health care innovation?
- Will this have adverse impact on actual healthcare?

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

Strategy Issues

- Companies used to want to “avoid” HIPAA where feasible – is that still the approach?
- Would you enter a market for a health app (and is this concern “good” for health care)?
- How would you address the FTC Chair statements on AI?
- Will “new” state laws make this situation better or worse?
- Will a future federal privacy law make this situation better or worse?

Questions?

Kirk J. Nahra
Washington, D.C.
202.663.6128
Kirk.Nahra@wilmerhale.com
@kirkjnahrawork