WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

ciitizen

Health Care in the National Privacy Debate

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

Deven McGraw
Co-Founder & Chief Regulatory Officer
Ciitizen
deven@ciitizen.com
@healthprivacy

citizen

Our Presentation Today

- We are having a more active debate on national privacy legislation than at any point in the past 20 years
- Still a long ways away (probably), but lots of progress and some clear concepts emerging
- Health care role is very much up in the air
- While the health care privacy eco-system has been relatively settled for many years, it is now facing meaningful upheaval – and may not be getting enough attention in the national debate

ciitizen

Our presentation today

- We will focus on two general topics
- How should the role of the healthcare industry (both “traditional” elements and emerging “non-traditional” components) and health care information be addressed in the debate over a national privacy law?
- What lessons can be learned from the HIPAA experience for the national privacy debate?
- The overall health care industry - including any components that utilize health information or participate in health and wellness activities - should be more engaged in this debate than it is
- There are challenging issues, consistency concerns, opportunities and real risks across the health information eco-system

ciitizen

Health Care privacy

- The topic of health care privacy has never been more important
- The success of the overall health care system depends on use of data – how we address the core privacy issues will play an important role in the overall success of the health care system
- If you are interested in privacy law, you must focus on the health care rules. It is by far the most evolved set of privacy and security rules, with the most varied set of interested stakeholders and the most complicated set of balancing tests
- If you are interested in health care, you also need to understand the privacy rules
- There are important lessons from the HIPAA experience for the national privacy law debate

citizen

Health Care Privacy in the National Debate

- HIPAA Rules have set the benchmark for the traditional health care industry(doctors, hospitals and health insurers) for almost two decades
- Have created a standard for the traditional health care industry and consumers that has worked (mostly) well for both the industry and consumers
- Increasing challenges with the existing structure given a variety of changes in both the traditional health care industry and in the broader health information ecosystem
- While HIPAA still works well where it applies (although this may be a controversial statement), there are increasing situations where it doesn't fit
- And some situations – even in the core health care system – where it may not work well

HIPAA History

- Remember how we got here – HIPAA Statute focused on health insurance portability and then standard electronic transactions
- Left HHS with a blank sheet of paper on which to write rules – with the only mandate being who the rules apply to
- Coverage limited (essentially) to certain health care providers and health plans/health insurers
- So HIPAA has never been an overall health care privacy rule – applies to certain defined entities for certain information in certain settings

citizen

Health Care Privacy/Emerging Issues

- One example of ongoing concern and tension is the debate/discussion over patient access
- Critical goal of many in the health care system
- Current real time debate
- One of the issues being debated involves the limitations of the HIPAA rules – what do you do when one goal (patient access) runs into the HIPAA limitations (data security)
- Decisions so far have favored access over security

citizen

HIPAA NPRM

- Published on the last day of the last Administration
- Comment period now closed
- Provisions permitting/encouraging/facilitating more information sharing were driven (primarily) by specific policy interests of the previous administration—the desire to expand opportunities for “coordinated care” and “value based” care, and the idea that better information sharing would have led to better results in dealing with the opioid crisis
- Biden administration will review and decide which substantive provisions they want to keep and which they want to abandon or modify

Hot Topics – The HIPAA NPRM

- Should OCR modify the Privacy Rule to clarify the scope of covered entities' ability to disclose PHI to social services agencies and community-based support programs where necessary to facilitate treatment and coordination of care with the provision of other services to the individual? For example, if a disabled individual needs housing near a specific health care provider to facilitate their health care needs, to what extent should the Privacy Rule permit a covered entity to disclose PHI to an agency that arranges for such housing?
- Should OCR modify the Privacy Rule to provide a more clear regulatory permission for sharing protected health information with friends and family members when it is "in the best interests" of the patient?

ciitizen

HIPAA NPRM

- The concern, however, in almost all of these situations is that the sharing would be done in expanded situations without specific patient permission — where seeking patient permission would be feasible (at least some of the time) and would be the vehicle for sharing today.
- This means that these goals are not without privacy costs — the proposals represent reasonable choices to facilitate certain goals of the health care system, despite tensions with patient privacy.

citizen

HIPAA NPRM

- The tension is quite explicit in the NPRM.
- For example, “Nearly all commenters who identified as family members of patients agreed that in many cases more information related to an individual’s SMI [serious mental illness] or SUD [substance use disorder] should be disclosed to family caregivers, and shared personal stories about the devastating consequences—such as suicide, missed appointments, homelessness, and lack of continuity in treatment and medication—that occurred because of a lack of information disclosure.”
- At the same time, OCR is clear that “Commenters who identified as patients or privacy advocacy groups almost universally opposed modifying the Privacy Rule to expand permitted disclosures of information related to SMI and opioid use disorder or other SUDs.”

citizen

HIPAA NPRM

- "Many commenters expressed fear of family members and employers having access to this information, citing potentially adverse consequences, including fear of discrimination, abuse, and retaliation."
- In addition, HHS notes that "Many health care providers expressed concern about the chilling effect that increased disclosures would have on individuals seeking treatment for opioid use disorders and stated that the Privacy Rule is already flexible enough to permit the amount of disclosure needed to address the opioid epidemic."

ciitizen

Non-HIPAA Health Information

- A result of the history of the HIPAA statute – where coverage under the privacy and security rules was defined by health insurance portability and standard electronic transactions
- HIPAA has never been a general overall health care privacy rule
- There have always been gaps – but the gaps are growing and becoming more important to individuals and the broadly-defined health care ecosystem
- And the overall health care ecosystem is learning that there is 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) are having implications for health care issues

ciitizen

Non-HIPAA Health Information

- Continued expansion of tech companies into the health care space
- Enormous growth in mobile apps, wearables, health-related web sites, wellness program issues, technology firms in general, etc.
- General concern is volume of health relevant data that isn't regulated by HIPAA
- And lots of questions – in the media and otherwise – even when the data "probably" is regulated by HIPAA (e.g., enormous, scary publicity about Google's relationships with hospital systems)
- Raising issues for patients, businesses and others

ciitizen

The National Debate

- California law has re-invigorated the national privacy debate
- Combined with GDPR and various privacy/security “problems”
- Lots of Congressional hearings, briefings, white papers, stakeholder positions
- Developments in many states, but few additional laws beyond California (yet)
- Virginia law is in place

ciitizen

California and the National Debate

- Industry is concerned about California by itself
- Industry is concerned about other states passing “California-like” laws
- Some in industry are concerned about global issues and EU “adequacy” (and more significant now with the data transfer issues)
- Could lead to a US law – with preemption – but could be a “strong” or “weak” law
- With each new state law, the “baseline” for a federal law grows

ciitizen

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 doesn't generally cover employers and employee information
7. How can consumers, businesses and others deal with this?

citizen

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
- Not a recommendation but an alternative model

ciitizen

What is the Right Approach

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

citizen

HIPAA Approach

- Various key components of the rules where privacy interests are balanced with other goals, including overall operation of the healthcare system
- Privacy rule developed areas of “treatment, payment and healthcare operations” (TPO), where individual consent is presumed.
- Designed to facilitate overall operation of the healthcare system while still providing appropriate protections for privacy

HIPAA Approach

- Same approach with “public policy disclosures”
- Rules essentially provide that patient consent is irrelevant, because of the other public policy goals driving the provisions for these disclosures (public health, litigation, health care oversight, research, etc.).
- GDPR and CCPA have none of that nuance
- The NPRM highlights even more nuance
- HIPAA also plays a critical role in defining “de-identified” health information – creating a standard that is thoughtful and precise and balances privacy with overall health care goals

citizen

HIPAA as a Model

- Could HIPAA serve as a model in the national debate?
- What elements of HIPAA might “work” in national legislation?
- Are there “negative” elements of HIPAA (things that haven’t worked)?
- We have lots of experience under HIPAA – what can we learn from it?

citizen

Lessons

- Important lessons that can be learned from the HIPAA experience
- Use and disclosure concepts may be critical – can we find a way to apply the concepts of “TPO” to “everything else?”
- TPO is a “context” for health care – is that a model?
- Health care has not been much of a focus specifically in the ongoing debate
- May be the hardest challenge in terms of balancing overall variety of interests – will that translate?

citizen

So Where Are We Going on Health Care Privacy?

- Current national debate is not focused on health care
- Freestanding effort on healthcare privacy is not currently active (some minor exceptions)
- Health care is not being addressed thoughtfully in the current debate over a national privacy law
- Default position of much of the health care industry has been “carve us out of new law”

citizen

Health Care in the National Debate

- New provisions likely would “cover” “non-HIPAA health care data” (and entities)
- Could/will lead to different standards
- Overlap issue of pre-emption – would health care industry “want” to be covered if strong preemption of state law
- Or a national law could replace HIPAA (possible but unlikely) (A broader and important question of now a new national privacy law will deal with existing US sector specific privacy laws for health, financial services and education)

ciitizen

Impact of COVID-19 – Some lessons

- Has highlighted the impact of employee privacy issues – where (in the US) there are few direct privacy laws (and the ADA is now something privacy lawyers and privacy officers need to know)
- Has highlighted a “weakness” in privacy law. Most privacy law addresses respective rights of data subjects and the entities they interact with (e.g., a bank and its consumers)
- COVID-19 has added the issue of impact of data sharing on third parties – others who might be impacted. Not really part of our privacy model
- In US, also has highlighted that there is essentially no law about the monitoring of “other” people – visitors, contractors, service providers, guests, customers

citizen

Today

- Lots of activity – stakeholders defining positions, draft legislation in Congress, congressional hearings
- Proposed legislation and principles from many sources
- Still a long way to go – but lots of activity throughout the year – and expected to start again in 2021
- Expectation that privacy will continue to be a hot button issue in COVID-19 mitigation - with a focus on health care
- Wild card – COVID privacy bill leads to late privacy add-on law
- Second wild card – Recent Supreme Court case limiting FTC authority leads to a “FTC only” privacy law

citizen

Key issues for legislative debate

- Preemption
- Private right of action
- Existing federal laws (and whether they will still apply)
- Scope of Individual Rights
- Permitted disclosures vs. areas where permission from consumers is needed
- Enforcement
- Coverage of employee data/“business to business” data

citizen

Key issues for legislative debate

- Dealing with innovation
- Broad scope of personal data
- Special protection for “sensitive” data (and how is that defined)
- Intention towards international principles
- Discrimination/Artificial Intelligence/Algorithms?
- Data security issues?
- National data breach standard?

citizen

Key issues for legislative debate

- Regulation of data brokers in general
- Regulation of “de-identified” data
- Commercial use/disclosure restrictions
- Incentives to leverage for public benefit
- What other issues should be part of the debate?

ciitizen

Our prediction for federal privacy legislation

- Odds go up in 2021 and going forward – presumption is that a Biden Administration will be somewhat more interested in a privacy law but not a significant priority
- Some open issues because of Vice President Harris' role as California AG in the past
- Major driver will be the wild card of other states - If 3-5 significant states pass "California-like" laws, then industry will need to support a federal law
- Our prediction – a meaningful chance (more than 50-50) of a national privacy law during this presidential term
- Enormous open questions of what this law would actually do and how it would interplay with other state and federal laws

ciitizen

Things to watch for

- If states start to move, will anything follow California?
- Will another state “model” emerge as the prototype?
- How broad will the discussions be on a federal law/How many topics will be included?
- Will there be a compromise on preemption/private cause of action?
- What about discrimination/artificial Intelligence/algorithm issues?
- How will existing federal laws be addressed? (exempted, supplemented, replaced)

ciitizen

Questions?

Kirk J. Nahra
WilmerHale
Partner and Co-Chair of global Cybersecurity and Privacy Practice
Washington, D.C.
202.663.6128
Kirk.Nahra@wilmerhale.com
@kirkjnahrawork

Deven McGraw
Co-Founder & Chief Regulatory Officer
Ciitizen
deven@ciitizen.com
@healthprivacy

Thank You