May 1, 2020

Adapting Privacy Law to Today's Health Care System

Kirk J. Nahra
WilmerHale

Deven McGraw
Ciitizen

Privacy+ Security Forum

Speaker Information

Kirk J. Nahra
Partner, WilmerHale
Co-Chair, Cybersecurity and Privacy Practice

Deven McGraw
Chief Regulatory Officer
Ciitizen

OUR SESSION

- HIPAA Rules have been in effect for close to 20 years
- Have created a standard for the health care industry and consumers that has worked (mostly) well for both the industry and consumers
- But there are increasing areas of potential concern where the rules may not work, or need to be adjusted or need to be supplemented
- We will be discussing some of those issues and the future of health care privacy - and thinking about changes based on COVID-19

OUR PRESENTATION

- 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

OUR PRESENTATION

- We are going to look at some of the key issues and areas that are testing the current system for health care privacy
- We are going to look at patient access issues, and discuss how the system is adapting to this concern
- We will discuss the impact of COVID-19 and how the privacy rules are (or should be) adapting
- We will then move to a discussion of the evolving health care landscape, and discuss the need for evolution of the privacy rules for social determinants of health

OUR PRESENTATION

- Then we will discuss the true future of privacy law – how new laws can and should address these issues
- We will discuss for the health care industry covered by HIPAA, and for those who are not – and the benefits and detriments to these audiences from new rules
- We will look at some of the current models and then discuss how these issues may play out in state and federal legislation

HEALTH CARE PRIVACY

- HIPAA Rules have set the benchmark for the health care industry for almost two decades
- 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

HEALTH CARE PRIVACY

- You have heard about 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
- Final rules allow (or in the case of CMS rules, require) patient education

PATIENT ACCESS

- The HIPAA Privacy Rule has always required patient access to information held by doctors, hospitals, and health plans covered by HIPAA.
- Historically hard for patients to exercise
- OCR enforcing more robustly
- New federal regulations provide greater access capabilities, new penalties

PATIENT ACCESS UNDER HIPAA

- Broad in scope – all info in “designated record set”
- Patient can get in form/format they request (including by e–mail) as long as “readily producible”
- 30 day time limit (+ 1 30-day extension)
- Limited fees can be charged
- Can patient have info sent directly to an app?

NEW FEDERAL RULES REQUIRE APIs

- Certified provider electronic health record vendors must enable patient-facing apps to connect through open, standard APIs to get subset of data (enforced beginning August 1, 2022).
- Limited ability to screen apps prior to making them available.

NEW FEDERAL RULES REQUIRE APIS (2)

- Health plans overseen by CMS must adopt open, standard APIs to make claims & clinical data available to patient-facing apps by July 1, 2021.
- Plans required to educate patients on privacy issues; may ask app vendors to be transparent about data practices.

NEW "INFORMATION BLOCKING" RULES

Privacy+ Security Forum

- Apply to providers, certified EHR vendors, and health information networks.
- Any obstacles to patients accessing their data could be "information blocking."
- Some "safe harbors" – but whether fees can be charged for digital access by patients (or their apps) is suspect.
- Opens up ability for patients to get data from some business associates (those meeting definition of health information network).
- Entities covered by the rule are permitted to educate patients on privacy risks.

COVID-19 DEVELOPMENTS

- Always interesting to see how system handles new challenges
- New guidance from administration
- Permitted use of telehealth – waiver of security rule provisions
- Allows convenience of telehealth without need to be concerned about specific security rule compliance
- General goal of making treatment consultations easier for doctors and patients
- All good – promotes confidence and comfort
- Please still try to be smart (don't do the telehealth visit while you are at Starbucks or somewhere else out in public)

COVID-19 DEVELOPMENTS

- Additional Waivers - privacy notices, sharing with friends and family, requests for restrictions and confidential communications
- Not areas where there has been traditional enforcement- but there may be reasons to send a message
- Issue with restrictions and confidential communications – we have seen an increase in domestic violence already, this may run counter
- So flexibility, no concern about enforcement, still be smart

ANOTHER EXAMPLE – THE HIPAA RFI

Privacy+ Security Forum

- 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?

HIPAA RFI

- Are these changes necessary?
- How might they work?
- Can they fit into the current structure of the rules?

NON-HIPAA HEALTH INFORMATION

Privacy + Security Forum

- Continued expansion of tech companies into the health care space
- Enormous growth in mobile apps, wearables, health-related web sites, wellness program issues, etc.
- General concern is volume of health 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

MORE "NEXT GENERATION" ISSUES

Privacy+ Security Forum

- An emerging (and related) issue - bringing "outside" HIPAA information "inside" HIPAA
- CEs are gathering all kinds of data about their patients/customers/insureds from outside the health care system and using it for "health care purposes"

RECENT HEADLINES

"When a Health Plan Knows How You Shop." (New York Times)

- Health plan prediction models using consumer data from data brokers (e.g., income, marital status, number of cars), to predict emergency room use and urgent care.

HEALTH CARE "SOLUTIONS"

- 3 Main Possibilities
- Something specific for this non-HIPAA health care data
- Something that covers all health care data (a "general" HIPAA)
- A broader overall privacy law (with or without a HIPAA carve-out)

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 health care industry has been “carve us out of new law”

SOME THINGS TO THINK ABOUT

California Consumer Privacy Act – how is your health information protected?

1. HIPAA protected information (generally exempted from CCPA)
2. CMIA covered companies/information (generally exempted from CCPA)
3. Common Rule/Clinical Trials (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?
8. Is this the best approach?

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

HEALTH CARE IN THE NATIONAL DEBATE

Privacy + Security Forum

- Isolated “solution” to issue of “non-HIPAA health data” seems to have disappeared
- Health care industry – regulated by HIPAA – could be left alone (excluded from application of national law, as is largely true with California)
- New provisions could apply to HIPAA entities – in addition to HIPAA

HEALTH CARE IN THE NATIONAL DEBATE

- New provisions likely would “cover” “non-HIPAA health care data” (and entities)
- Could 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)

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

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

TODAY – Impact of COVID-19

- Obviously debate on overall privacy law has slowed to essentially nothing
- Some initiatives to pass COVID-19 specific privacy legislation (just starting this week)
- COVID-19 has altered the debate on public vs. private interests

TODAY – Impact of COVID-19

- 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)
- What about the monitoring of “other” people – visitors, contractors, service providers, guests, customers

TODAY – A PREDICTION

- No national privacy legislation in this Congress (had always been unlikely, now essentially zero chance)
- Expectation that privacy will continue to be a hot button issue in COVID-19 mitigation - with a focus on health care
- Reasonable likelihood of some short-term or emergency privacy legislation – Will this become permanent (compare telehealth guidance)

TODAY – A PREDICTION

- Still a reasonable expectation of national privacy legislation during next presidential term – regardless of who is president
- Major driver of the speed of this debate (aside from COVID-19) 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

TODAY – A PREDICTION

- Increasing recognition of unique challenges related to health care privacy
- Also a recognition that many of these issues are outside of HIPAA's scope
- Health care industry has (so far) been largely passive in this debate
- Meaningful risk that health care privacy in a new law will be driven by people outside of health care

QUESTIONS

Kirk J. Nahra
WilmerHale
202.663.6128
kirk.nahra@wilmerhale.com
@kirkjnahrawork

Deven McGraw
Ciitizen

deven@ciitizen.com