Making Sense of the New World of Health Care Privacy

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

Sheila Sokolowski
Hintze Law PLLC
Chicago, IL
872.310.4062
Sheila@hintzelaw.com
@SMSokolowski

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

Hintze Law
Privacy + Data Security

Our Presentation Today

- The health care privacy field has been relatively stable for many years - but now is increasingly unstable and complicated
- The HIPAA framework is still key and is evolving, but more and more of the field involves other laws
- This meaningful upheaval may be creating a bad situation for both consumers and health care businesses
- The national privacy debate presents some opportunities to address these issues, but health care has not been getting enough attention in this debate

Hintze Law
Privacy + Data Security

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

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

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?

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.

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."

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."

Hot Topics - Health Information Security

Ransomware attacks targeting healthcare organizations

- 2020: 92 attacks, 600+ providers and 18+ million patient records - $2+ million in ransom
- As of May 2021: 82 attacks, 48 targeting US 60 percent increase over 2019
- Attack on Irish Health System (May 2021)
  - Affected every aspect of clinical care
  - Forced to use pen and paper documentation
  - Patient data released online
  - Same ransomware (Conti) attacked health systems in the US
  - Triple extortion– data is encrypted, exfiltrated and data leak
- DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks | CISA
- Conti Ransomware Attack Impact Healthcare and First Responder Networks | FBI
- Indicators of Compromise Associated with Hive Ransomware | FBI

Health Information Security

CA AG Bulletin: *Obligation to Proactively Reduce Vulnerabilities to Ransomware Attacks and Requirements Regarding Health Data Breach Reporting*

- CMIA and HIPAA require security measures to prevent the introduction of malware and protect health information from unauthorized use or access.
- Minimum preventive measures
  - Latest security patches
  - Virus protection software
  - Training on suspicious weblinks and phishing emails
  - Restrictions on unapproved software
  - Maintain and test backup and recovery plan
  - Monitor advisories from government agencies
- Comply with CA breach notification law

Health Information Security

Class action lawsuits alleging failure to:

- Properly monitor its data security systems for intrusions, brute-force attempts and clearing of event logs;
- Apply all available security updates, install the latest software patches, update its firewalls, check user account privileges or ensure proper security practices;
- Practice the principle of least-privilege and maintain credential hygiene;
- Avoid the use of domain-wide, admin-level service accounts and employ or enforce the use of strong randomized, just-in-time local administrator passwords;
- Properly train and supervise employees in the proper handling of inbound emails.

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

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

Non-HIPAA information

FTC Statement On Breaches by Health Apps and Other Connected Devices

- Breach of security includes disclosure of sensitive health information without users' authorization.
- Health apps furnish health care services or supplies and thus are a health care provider.
- Health apps are covered if they collect information directly from consumers and have the technical capacity to draw information from another source.

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?

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

Hintze Law
Privacy + Data Security

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

COVID-19 and its implications for Privacy Law

Early stages (spring 2020) – what can I disclose about an employee that tested positive?

First – **this is not a HIPAA issue** (repeat)

Some relevance of the ADA – not usually thought of as a privacy law

Evolving guidance

In general, led to thoughtful and responsible disclosures

COVID-19 and its implications for Privacy Law

Second Phase - Contact tracing

Also not HIPAA (do you sense a theme here?)

Privacy concerns front and center

Third Phase – Collection of vaccination information

Still not HIPAA

Impact of COVID-19 – Some lessons

The "patchwork quilt" becomes a "tangled fishing net."

- *EEOC: employers may request proof of vaccine status.*
- *ADA: keep employee medical information confidential and separate.*
- *OSHA: the vaccine card is a medical record and copy given to employer must be retained for employment plus 30 years.*
- *CCPA and CPRA: vaccine status is personal information.*
- *At least one state, Montana: vaccine status is protected.*
- *Santa Clara County Health Department: all businesses and government entities required to determine vaccine status of employees.*

Impact of COVID-19 – Some lessons

Ireland DPC:

> ……[I]n the absence of clear advice from public health authorities in Ireland that it is necessary for all employers and managers of workplaces to establish vaccination status of employees and workers, the processing of vaccine data is likely to represent unnecessary and excessive data collection for which no clear legal basis exists.

UK ICO:

> A person's COVID status is special category data, as it is their private health information. Your use of this data must be fair, relevant and necessary for a specific purpose.

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

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

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?

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"

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)

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 heath care industry needs a position if the exemptions do not continue

Does the health care industry want this fragmented field going forward?

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

Sheila Sokolowski | Partner and Chair Health and Biotech Privacy Group
Hintze Law PLLC
Chicago, IL
872-310-4062
Sheila@hintzelaw.com
https://hintzelaw.com/
@SMSokolowski

Hintze Law
Privacy + Data Security

Thank You