TEMPUS

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

How Privacy Law Can Help (or Hurt) Health Care

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

Robyn Eckerling
Chief Privacy Officer
Tempus
Robyn.eckerling@tempus.com

TEMPUS

Privacy and Security for Health Care

- Most evolved structure for privacy and security in the US
- A good case study for the full range of issues that arise for businesses, consumers, regulators and policymakers
- Primary focus is on HIPAA and its core obligations

TEMPUS

For Your Consideration

- The challenges presented by privacy and security in a data driven health care world may create one of the most important challenges we face in the health care system
- How we resolve these issues will impact the success of our health care system in significant ways going forward

TEMPUS

Health Care Privacy Debates

- Health care field may raise the most complicated array of legal and policy issues in the privacy space, given the interests of individuals, patients, governments, employers, taxpayers and society at large
- Anyone thinking about health care has to be analyzing the impact of privacy law
- Anyone thinking about privacy law has to understand the health care example

TEMPUS

Health Care Privacy

- Is there really something “different” about health care information in general or any particular kinds of health care information
- What happens if this data is not treated differently
- How do we deal with the evolving views on what kinds of data is ”relevant” to health, and how this (not obviously health) data should be treated – shopping habits, voting patterns, television viewing, income, etc.

TEMPUS

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. Voting Records/Purchasing Habits/Television Watching (used to evaluate medical issues)

TEMPUS

HIPAA

- **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct (1996)
- Focused on portability of health insurance
- Then focused on “administrative simplification” (standard transactions)
- Only then got to privacy and security, with almost no detail

TEMPUS

HIPAA

- Statute did not focus on privacy or security
- HHS essentially had to write rules from scratch
- Primary impact of statute on the rules involved who the rules could be applied to – this is really the only "relevant" impact of the HIPAA statute on privacy and security.

TEMPUS

HIPAA

- HIPAA has never been an overall health information privacy law - A result of the statutory history
- Applies to certain information held by certain people in certain situations
- Mainly doctors, hospitals, health insurers and their service providers
- Rules were mainly policy choices to promote privacy and security while still allowing for an effective health care system

TEMPUS

Core principles of use and disclosure (A key policy choice)

- Use and disclosure rules for covered information is a key element of any privacy law – what you can do with the personal information
- HIPAA premise is to make it relatively easy for key health care purposes and harder for everything else
- Driven by policy

TEMPUS

Core principles

- Use and disclosures for TPO (**T**reatment, **P**ayment and Health Care **O**perations) purposes – presumed patient consent
- Core elements of the health care system – relatively easy (with appropriate protections)

TEMPUS

Core Principles

Goal here is strong privacy protection while still allowing system to work well – which benefits industry and consumers and the broad range of audiences

Also national priority purposes, where health care system goals drive rules

TEMPUS

The evolving system

HIPAA generally works well where it applies (some debate about this)

Certain areas where the system is evolving - even within HIPAA – to raise questions

TEMPUS

Hot Topics – The HIPAA RFI/Potential 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?

TEMPUS

HIPAA NPRM

- Published on last day of last Administration
- Presumably will be slowed/modified by Biden Administration – not because they are opposed but because they will want to review
- Provisions permitting/encouraging/facilitating more information sharing are driven (primarily) by specific policy interests of the last 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.

TEMPUS

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 (along with broad provider discretion).
- 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

TEMPUS

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."

TEMPUS

HIPAA NPRM

- 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."

TEMPUS

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.”

TEMPUS

HIPAA Approach

- De-identification in the HIPAA rules represents one of the many choices made by HHS in developing the rules
- Various key components of the rules where privacy interests are balanced with other goals, including overall operation of the healthcare system

TEMPUS

Key HIPAA Principles

- Very restricted use and disclosure rules for PHI
- PHI can be “de-identified” under specific detailed rules
- Once PHI has been de-identified, it is no longer subject to the HIPAA rules

TEMPUS

Key HIPAA Principles

- HIPAA permits you to do anything with de-identified data
- This was not an automatic rule – HHS could have said something different, or reduced the general HIPAA restrictions
- This “unrestricted” environment is one reason this information is so valuable – can be sold, used for research or for any other purpose under current law.

TEMPUS

HHS Comments

- Although these approaches (*NOTE – a zero-risk approach)* would provide a marginally higher level of privacy protection, **they would preclude many of the laudable and valuable uses discussed** in the NPRM and would impose too great a burden on less sophisticated covered entities to be justified by the small decrease in an already small risk of identification.

TEMPUS

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

TEMPUS

Non-HIPAA Health Information

- What is “outside” of HIPAA is growing
- Web sites gather and distribute healthcare information without the involvement of a covered entity (from commercial web sites (e.g., Web MD) to patient support groups to the growth of personal health records).
- Wearables
- Mobile apps

TEMPUS

Non-HIPAA (and non-health?)

- 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”

TEMPUS

Structural reminder

- Why does this matter?
- Not all health information – only health information that has a defined connection to a “covered entity” (typically a health care provider or health insurer/health plan)
- Think wearables/Apple Watch/Fitbit/mobile apps
- No covered entity involved
- Lots of individual health information
- No HIPAA coverage

TEMPUS

Structural reminder

- Now think Apple/Aetna
- Apple and insurance giant Aetna have teamed up on an iPhone and Apple Watch app that provides rewards, including an option to earn a free Apple Watch, to members who engage in healthy behaviors like getting regular exercise and more hours of sleep. The new app also provides Aetna members who sign up with nudges, such as to get an annual flu shot or take their medication on time.
- What about an employer offering this?

TEMPUS

Where Do We Go From Here with Health Care Privacy?

- COVID-19 Questions
- Balance between patient interests (convenience vs. privacy)
- Balance between privacy interests and health care system interests
- How to address non-HIPAA health data issues (health data not a part of the HIPAA regulatory framework – e.g., employee health data)
- How to address data that isn't about your health but that is relevant to the health care system (e.g., location data used for health care monitoring)

TEMPUS

The Future: What is the Right Approach

- Should there be an “overall” approach to 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

TEMPUS

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?

TEMPUS

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

TEMPUS

Example 1

- Hospital is engaged in cutting edge cancer treatments, About a dozen other hospitals around the country are involved in the same treatments.
- Vendor wants to collect data from each of the hospitals to analyze across the broader data set
- Vendor will develop artificial intelligence models to help physicians evaluate treatment options
- Vendor will sell the AI models to hospitals who do not participate in the data analytics activity

TEMPUS

Additional Examples

- Access/Security (tensions)
- Telehealth (during COVID and otherwise)
- Medical research (does HIPAA help or impede medical research?)

TEMPUS

Healthcare Privacy—Opportunities and Challenges

- Cost of Cloud Computing has dropped dramatically
- De-Identified Data
  - Clean structured data in one place allows for meaningful analysis
  - Discovering better ways to treat patients through data
- Artificial Intelligence
- Balance between patient interests (convenience vs. privacy)
- Balance between privacy interests and health care system interests
- How to address non-HIPAA health data issues (health data not a part of the HIPAA regulatory framework – e.g., employee health data)
- How to address data that isn't about your health but that is relevant to the health care system (e.g., location data used for healthcare monitoring)
- Responsible use of data

TEMPUS

Questions?

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