Privacy Topics for Digital Health Entrepreneurs: HIPAA, CCPA and COVID-19

Presented by Tracy Shapiro and Haley Bavasi

May 7, 2020

WILSON
SONSINI

Welcome! Thank you for joining us.

Regulated Data and the Implications for Digital Health

HIPAA for Digital Health Entrepreneurs

CCPA for Digital Health Entrepreneurs

HIPAA and CCPA: Where one begins and the other ends…

Privacy Legislation and Regulatory Enforcement in the Time of Coronavirus

WILSON
SONSINI

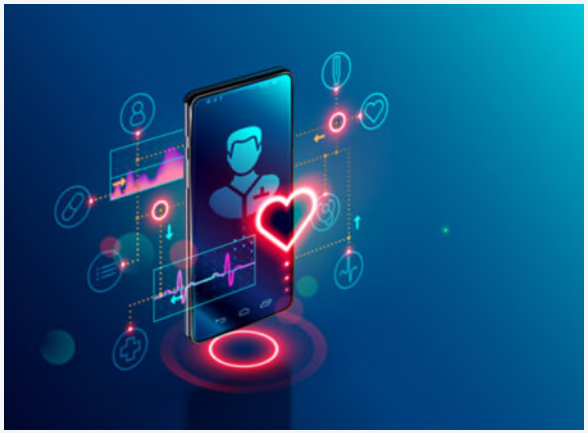
Intersections of Data x Privacy x Digital Health

However you choose to define it, the “digital health” star has been rising for decades. In this particular moment, however, the singular importance of enabling access to health care services through remote, technology-enabled platforms may have irreversibly catapulted digital health, in all its myriad forms, to the status of “new normal” in a post-Covid era.

What is "digital health"?

The definition we'll put forth is the convergence of technology, often with big data and analytics, with the purpose of promoting innovation in health outcomes, care, delivery and payment

- Consumer-Driven Health & Wellness, e.g.
  - Wearables and connected devices (e.g., FitBit, smart scales, continuous glucose monitors)
  - DTC testing (e.g., 23andMe)
  - Mobile health (mHealth) (e.g., diet tracking and lifestyle Apps)
- Provider, Payer and Employer-Driven:
  - Telehealth and telemedicine
  - Health IT, including analytics (e.g., ML/AI driven Clinical Decision Support software and SaMD)
  - Electronic Health Records
  - Value-based care tools
- Industry Driven Products and Research, e.g.,
  - Software as a Medical Devices (SaMD)/ Remote monitoring devices
  - Machine Learning and AI used for Drug Discovery
  - Precision medicine
  - Digital Therapeutics
  - Clinical Trial recruitment
- To name a few…



Transacting in Regulated Data

Because data is core to the digital health industry, we have to navigate the complex web of privacy and data security regimes

- Under which legal regimes might the data regulated?
  - HIPAA and CCPA Challenges
- What are the data flows and how do they implicate these different regimes at different times?
- How and where is the data hosted?
- How is it used to perform the services?
- Does the company have a secondary use strategy for the data? E.g.:
  - Train their algorithms?
  - Data monetization?
  - Product improvement?

The Alphabet Soup of Regulated Data

Data can of course be regulated by a variety of legal regimes, including:

- **CCPA** – California Consumer Privacy Act (California)
- **COPPA** – Children's Online Privacy Protection Act (Federal)
- **FERPA** – Family Education Rights and Privacy Act (Federal)
- **FTC** – Federal Trade Commission
- **GDPR** – the General Data Privacy Regulation (EU)
- **GLBA** – Gramm-Leach-Bliley Act (Federal, applies to financial institutions)
- **HIPAA** – Health Insurance Portability and Accountability Act (Federal)
- Various US state laws and ex-US legal regimes

WILSON
SONSINI

Overview of the Health Insurance Portability and Accountability Act of 1996 – AKA "HIPAA" – For Digital Health Entrepreneurs

HIPAA Roadmap

- Broad overview of the law
  - HIPAA Privacy Rule
  - HIPAA Security Rule
  - HIPAA Breach Notification Rule
  - HIPAA Enforcement Rule
- Who is covered by HIPAA?
  - Covered Entities
  - Business Associates
- Protected Health Information
- Coronavirus Notice of Enforcement Discretion

Why HIPAA?

- While best known as a law about privacy and security, HIPAA is much broader
- Back when Congress functioned, HIPAA was passed as a way to improve efficiency and effectiveness of health care system
  - In mid-late 90's, could see health care system rapidly moving from analog-paper based institution into the digital era
  - HHS was directed to adopt national standards for electronic code sets
- National Provider Identifier (NPI) system adopted, which allows providers to bill federal and private insurers
- HIPAA does LOTS of cool things that allow an incredibly complex system to run [more] smoothly!

Why HIPAA? Cont'd

- Concern, too, that advances in technology could erode privacy and compromise security → HHS was also directed to adopt Federal privacy protections and security standards for certain individually identifiable health information
- Also a concern that individuals should be able to move seamlessly between jobs, health insurers, and providers, and have their health information follow → that's why "P" stands for "Portability" (because who hasn't wondered about that??)

The Rules

There are four "Rules" – Privacy, Security, Enforcement and Breach Notification

Privacy Rule

- First final Privacy Rule published in 2000. Sets national standards for the protection of individually identifiable health information by covered entities (health plans, health care clearinghouses, and health care providers who conduct standard health care transactions electronically) and now their business associates. (45 CFR Parts 160 and 164)

Security Rule

- First final Security Rule in 2003. Sets national (but flexible) standards for protecting the confidentiality, integrity and availability of electronic protected health information. (45 CFR Parts 160 and 164)

The Rules

There are four "Rules" – Privacy, Security, Enforcement and Breach Notification

Enforcement Rule

- Went into effect 2006. Provides standards for the enforcement of all the Administrative Simplification Rules (think of that as HIPAA). (45 CFR Part 160, Subparts C, D and E)

. . .

[**HITECH**]

Is not a Rule, but, because we're exploring this chronologically, it's time to flag the passage of HITECH

Health Information Technology for Economic and Clinical Health Act ("HITECH")

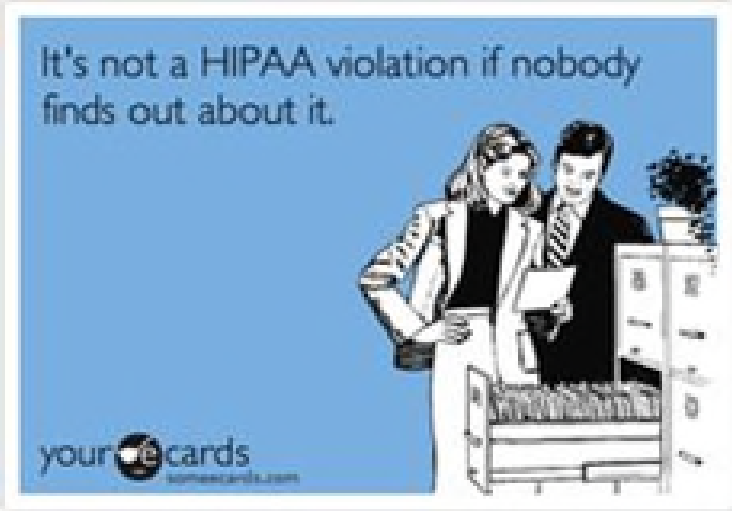
- Part of the American Recovery and Reinvestment Act (ARRA) of 2009 (during the recession). Primarily a vehicle to incentivize rapid adoption of health care IT generally through creation of national health care infrastructures, and specifically through driving adoption of EHRs by providers
- However, it also broadened the scope of privacy and security protections under HIPAA, INCLUDING, very importantly, extending the obligation to comply with the Rules to all business associates (not just covered entities)

The Rules

Back to regularly scheduled programming…

Breach Notification Rule

- Issued as part of the Final Omnibus Rule, which implements a number of provisions of the HITECH Act. Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information (PHI)



Who is Covered by HIPAA?

HIPAA applies to:

- **Covered Entities**
  - Health care providers
  - Health plans
  - Health care clearinghouses
- **Business Associates**
- **Subcontractors** of business associates

Covered Entities

Health Care Provider	Health Plan	Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies But only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.*	This includes: • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, e.g. Medicare, Medicaid and the military and veterans health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa

***What does this mean??** *A "standard for which HHS has adopted a standard" is also called a "standard transaction" – these are defined at 45 CFR 160.103 (definition of "transaction"); administrative requirements for standard transactions are at 45*

Business Associates

Business Associates are entities that provide certain services to covered entities or other business associates (in the latter case, they are a "subcontractor")

- The majority of our digital health entrepreneurs provide a **product or service**. So, if they are in the health care or life sciences industry, they might be a business associate depending on their customer.
  - **Is your customer a health care provider or health plan?** **NOTE**:
    - The definition of "health care provider" is very broad (e.g., as just discussed, including a medical device manufacturer if they do more than just ship the product off the shelf when selling it)
    - If you have an "employer" customer, check if it is actually an employer self-insured group health plan, as these are covered entities (separate from the employer itself)
- **OR, are you providing services directly to consumers? (and not on behalf of a covered entity)**

Business Associate Defined

- Because the consequence of being a business associate v. not being one are complying v. not complying with HIPAA, it's important to understand this distinction
- Seeing cases come up where "on behalf of" without disclosure of PHI being contested by customer as creating BA relationship
- **Important note**: whether a business associate agreement is in place is NOT dispositive of whether or not you are a business associate:
  - If you know or should have known you are receiving PHI, you have 3 options within 30 days:
    - Become HIPAA compliant
    - Return the PHI
    - Destroy the PHI with permission from covered entity

Definition of Business Associate (45 CFR 160.103)		
A business associate means, with respect to a cover entity (other than as a member of the workforce) **a person who, on behalf of such covered entity**:	**Creates, Receives, Maintains, or Transmits Protected health information**	For a **function regulated by this subchapter** (see definition of "health care operations", 45 CFR 164.501)
OR:	Provides **legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services**	**To a covered entity**, and
		Where **the provision of the services involves the disclosure of protected health information**

Protected Health Information

- As noted previously, not recommended to start analysis of HIPAA applicability thinking about PHI, but must think about/double-check analysis of data through PHI lens by looking at definition.
- Get to definition of "PHI" through "individual identifiable information"

Definition of Protected Health Information (45 CFR 160.103)			
Protected Health Information means:	**Individually identifiable information** that is:	Transmitted by electronic media	
		Maintained in electronic media	
		Transmitted/maintained in **any other form or media**	
Individually Identifiable Information is a **subset of health information** that is:	**Created or received by a health care provider, health plan, employer or a health care clearing house**, and:	Relates to the **past, present, or future** physical or mental health or **condition** of an individual; the **provision of health care** to an individual; or the past, present, or future **payment** for the provision of health care to an individual; and:	That **identifies** the individual, or
			With respect to which there is a **reasonable basis** to believe the information can be **used to identify** the individual.

How Can PHI be Used and Disclosed?

Covered entities can Use and Disclose (defined term) PHI for treatment, payment and operations ("TPO")

- The TPO buckets are categorically defined under the Rules
- Research is not part of TPO and requires patient authorization if it is not a Use or Disclosure that is "preparatory to research"*

Business associates may only use PHI consistently with the underlying services agreement, and that agreement must be within the scope of TPO

- i.e., the covered entity can't direct a BA to Use or Disclose PHI in a manner it itself could not do

Alternatives for Obtaining Data

IF:

(1) There is no BAA in place (because no business associate services are being provided), and the information sought is PHI,

OR

(2) The Use or Disclosure is for a purpose that is not TPO

You need:

- → Patient authorization needs to be obtained for full-on PHI (*note if you hear client talk about "consent", reach out to Haley*)
- → A Limited Data Set could be obtained through signing a Data Use Agreement
- → De-Identified Data (but someone else has to do the de-identification unless you are a BA with permission)
- → One of the narrow exceptions under 45 CFR 164.512 (Uses and disclosures for which an authorization or opportunity to agree or object is not required)

HIPAA in the Time of Coronavirus

OCR has issued a "Notice of Enforcement Discretion for remote communications during the COVID-19 nationwide public health emergency"

- Essentially advises HIPAA-covered healthcare providers (HCPs) that OCR, which is responsible for enforcing certain privacy and security regulations under the Act, will not seek any enforcement against HCPs who use communications technologies to connect remotely with patients, even if such technologies "do not fully comply" with the requirements of the HIPAA rules
- HHS expressly states the Notification applies to telehealth provided for any reason, not just treatment of conditions related to COVID-19
- Accordingly, HCPs are presently permitted to use any *non-public* communication technology to provide telehealth to patients during the COVID-19 emergency. HHS will suspend its enforcement for noncompliance with the HIPAA Rules in connection with the "good faith provision of telehealth."

HIPAA in the Time of Coronavirus

Other HHS Actions/Existing Regulations:

- Effective March 15 and retroactive to March 1, HHS Secretary Alex Azar issued a Section 1135 waiver of sanctions and penalties for noncompliance with particular provisions of the HIPAA Privacy Rule for any hospital that has activated its disaster protocol
- There are other allowance for disclosures of protected health information (PHI) for public health purposes that are not specific to the COVID-19 emergency, but always in effect. With respect to public health activities, covered entities and business associates may disclose protected health information as needed without an individual's authorization under the following conditions
  - To a public health authority
  - At the direction of a public health authority to a foreign government agency
  - To individuals at risk of contracting or spreading disease
- See client alert here: https://www.wsgr.com/en/insights/hipaa-and-covid-19-update-hhs-and-ocr-remove-barriers-to-accessing-and-providing-telehealth-services-and-other-waivers-in-midst-of-covid-19-emergency.html

Return to Work – Public Health Disclosure under 45 CFR 164.512 (Uses and disclosures for which an authorization or opportunity to agree or object is not required):

(b) *Standard: uses and disclosures for public health activities*—(1) *Permitted disclosures.* A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer:

(*1*) To conduct an evaluation relating to medical surveillance of the workplace; or

(*2*) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(*1*) By giving a copy of the notice to the individual at the time the health care is provided; or

(*2*) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.


HIPAA HIPPO
IS DISPLEASED WITH YOUR HANDLING OF PROTECTED HEALTH INFORMATION


THE HIPAA HIPPO SAYS
BECAUSE WE CARE, WE'RE HIPAA AWARE.
memegenerator.net


WHAT ANIMAL IS GREAT AT KEEPING SECRETS?
A HIPAA-POTAMUS

YES!!!!!!


HIPAA HIPPO, IS IT OK THAT I LISTEN TO "SAFETY DANCE" WHILE I DO MY HIPAA TRAINING?
YES
memegenerator.net


HIPAA-POTAMUS IS DISAPPOINTED
THAT YOUR EMAIL CONTAINED PHI
memegenerator.net


HIPAA HIPPO
IS NOT AMUSED YOU MISSPELLED HIPAA

WILSON
SONSINI

The California Privacy Protection Act – AKA "CCPA" – for Digital Health Entrepreneurs

CCPA at a Glance

What is it, and why is it a big deal?

- Game-changing privacy law that broadly applies to businesses (that meet certain numbers thresholds) that collect personal information about California residents
- Substantial new privacy rights for Californians
- High potential fines for privacy violations
- Class action liability + statutory damages for data breaches

What's the status?

- Effective January 1, 2020
- Privacy provisions enforceable by the California AG July 1, 2020
- Data breach private right of action available January 1, 2020
- Awaiting final AG regulations (latest draft: March 11, 2020)

Key CCPA Components

Transparency Requirements

- Privacy policy requirements
- "Notice at Collection"

Right to Access & Delete Personal Information

- Specific Piece of Personal Information
- Information about Categories of Personal Information

Right to Opt Out of Sale of Personal Information

- "Sale" broadly defined to include any disclose of PI in exchange for monetary or valuable consideration
- "Do Not Sell" link on homepages

Consent to Sell Minor's PI

Non-Discrimination and Incentives

Operational Impacts and Considerations

Know Your Data: Identify, inventory, and map data flows at a level sufficient to meet CCPA requirements

Privacy Disclosures: Inventory and update privacy policies and UI

Implement Opt-Out Requirements

- Create opt-out mechanism
- Post "Do Not Sell My Info" link

Vendor and Third Party Management

Establish Processes and Mechanisms for Access & Deletion Requests

Assess Security Measures and Breach Risks

CCPA & HIPAA – Where One Begins and the Other Ends

The CCPA does not apply to:

- Protected Health Information (PHI) that is collected by a covered entity or business associate governed by HIPAA, or Medical information governed by California's Confidentiality of Medical Information Act (CMIA).
- Patient information that a "Covered Entity" governed by HIPAA or a "provider of health care" governed by CMIA maintains in the same manner as PHI or Medical Information.
- Information collected as part of a clinical trial that is subject to federal HHS and FDA regulations for the protection of human subjects

CCPA & HIPAA – Where One Begins and the Other Ends

"I'm a Covered Entity (or Business Associate) handling PHI. So that means I don't have to worry about CCPA?" Not so fast...

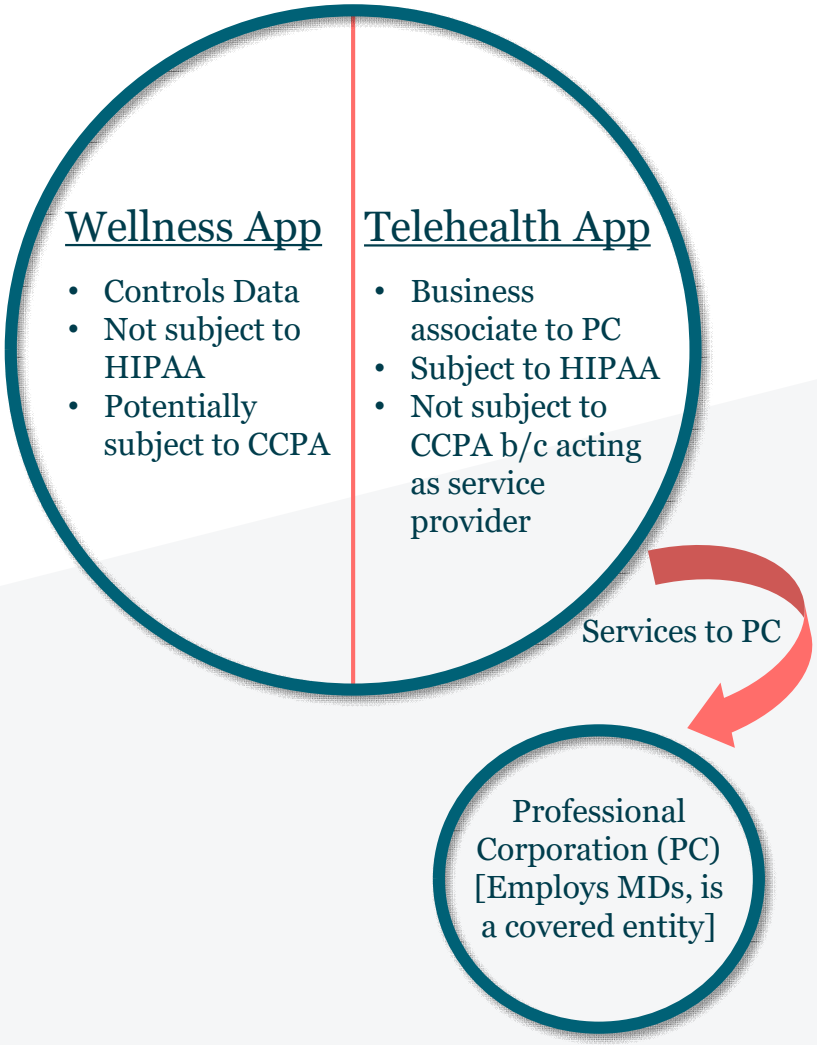
Covered Entities and Business Associates commonly handle individual information that may not be considered PHI or Medical Information. Examples:

- Website cookie data
- Website form to receive more information about product/service
- Physician data (that is not connected to a patient record)
- B2B data (e.g., Customer data like information maintained by a health plan's customers versus insured members)
- HR data
- De-identified Data

Hybrid Model – Data Controller and Business Associate

Just because part of your product or service renders you a business associate, does it in all instances?

- Consider the example of a wellness + telemedicine platform where the company is operating as a business associate when carrying out part of the services, and controlling the data in another.
- In these kind of hybrid platforms, CCPA could apply to some of the data, and not to other of the data



CCPA in the Time of Coronavirus

Delayed Enforcement?

- In late March a coalition of 60 US companies, including the California Chamber of Commerce, sent a letter to CA AG Javier Becerra urging him to delay enforcement in light of: (1) The Covid crisis; and (2) The lack of regulations.
- Becerra responded that enforcement will not be delayed.

Data Processing for COVID-19

- Employee monitoring of remote working
- Employer return-to-work issues
- Contact tracing

WILSON
SONSINI

Privacy Legislation and Regulatory Enforcement in the Time of Coronavirus

Privacy Legislation in the Time of Coronavirus

COVID-19 Consumer Data Protection Act of 2020

- Introduced by Wicker (Chair of Commerce Committee), Thune, Moran, Blackburn
- Covered entity must provide an individual with notice and obtain affirmative express consent to collect, process, or transfer "covered data" for one of the following purposes: (1) To track the spread, signs, or symptoms of COVID–19; (2) To measure compliance with social distancing guidelines or other requirements related to COVID–19 that are imposed on individuals under a Federal, State, or local government order; OR (3) To conduct contact tracing for COVID–19 cases.
- "Covered Data" = precise geolocation data, proximity data, and health data
- Also includes public reporting obligations, an opt-out mechanism, data deletion or de-identification obligations, and security requirements
- Potential sticking points: preemption of state laws + no private right of action

Privacy Enforcement in the time of Coronavirus

Congressional Inquiries

- Markey Inquiry Letters

Potential FTC or State AG Enforcement

- Advertising/Marketing warning letters
- Potential privacy investigations?

WILSON SONSINI

Thank you!

Tracy Shapiro
tshapiro@wsgr.com
206-883-2662

Haley Bavasi
hbavasi@wsgr.com
206-883-2662