

# Leveraging Health Data and Digital Health Technologies: Opportunities and Challenges

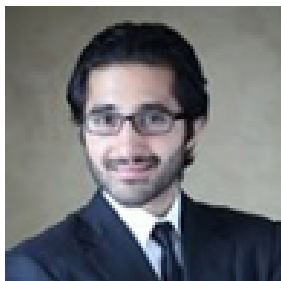
March 25, 2022

Mohammad Amer  
Joanne Charles  
Kezia Cook-Robinson  
Elliot Golding



# Today's Presenters

---



**Mohammad Amer**  
Senior Privacy Counsel  
Genentech



**Joanne Charles**  
Senior Corporate Counsel  
Microsoft



**Kezia Cook-Robinson**  
Senior Privacy Counsel  
Verily



**Elliot Golding**  
Partner, Squire Patton Boggs  
(Washington, DC)

- 
- Federal Statutes / Rules
  - Federal Authorities Regulating Health Data
  - State Statutes
  - State Authorities Regulating Health Data
  - Analysis Basics
  - Practice Scenarios
  - Questions

# *Legal Landscape for Health Data: Federal Statutes / Rules*

---

- HIPAA (including HITECH)
- 42 CFR Part 2 (substance use disorder)
- ONC Information Blocking and CMS Interoperability Regs
- Federal Trade Commission (FTC) Act Section 5 Authority
- Common Rule (and equivalents)
- Other (COPPA, FCRA, GLBA)
- Government program rules (Medicare, Medicaid, federal/state exchanges)
- **Guidance from Federal Regulators:**
  - HHS Health App Use Scenarios
  - HHS Cloud Computing Guidance
  - SAMHSA Part 2 Guidance

# Federal Authorities Regulating Health Data

Office of Civil Rights (OCR)	General Services Administration (GSA)	Substance Abuse and Mental Health Services Administration (SAMHSA)	Office of National Coordinator for Health Information Technology (ONC)
Food & Drug Administration (FDA)	Federal Trade Commission (FTC)	Office for Human Research Protections (OHRP)	
Centers for Disease Control & Prevention (CDC)		Office of the Inspector General (OIG)	Centers for Medicare and Medicaid Services (CMS)

# *Legal Landscape for Health Data:*

## *State Statutes*

---

- Privacy, security, breach notification and data retention / destruction
- State laws governing medical information and sensitive services
- California Consumer Privacy Act/California Privacy Rights Act
- Virginia Consumer Data Protection Act
- Colorado Privacy Act

# State Authorities Protecting Health Data

State Courts	Medicaid		State Certifications
	Health Boards	Medical Boards	
Attorneys General		Licensure	State Pharmacy Board

# Analysis Basics

## Data Flow Decision Points

<b>Where to start?</b>  <b>What privacy laws might apply?</b>	What personal data is involved?	What is my client's role in this data processing?	Who is the data subject?  (e.g., patient, research participant)
	Is the data identifiable?  (consider if De-identified Data vs. Limited Data Set)	What is the data source?  (e.g., data broker, research study, government, CE/BA)	What is the use case / purpose (primary and secondary) of this data processing?  (e.g., research)
	Is the data "sensitive"?  (e.g., Part 2 data?)	Who is the data recipient, and how will recipient use the data?  (e.g., is it a "sale"?)	What jurisdictions apply?  (consider if jurisdiction has equivalent of federal privacy laws – e.g., HIPAA and CMIA)



# Analysis Basics:

## Additional Considerations

<p>What authorizations are required?</p> <p>(e.g., HIPAA, Part 2)</p>	<p>What kind of agreements are required?</p> <p>(e.g., Data Use Agreement, BAA, Non-Disclosure/Data Sharing Agreement, HIE Participant Agreement)</p>	<p>Does this health-related data require heightened security?</p>
<p>What privacy notice (external representations about data practices) applies and does this data processing align with the privacy notice?</p>	<p>What data retention requirements apply?</p>	<p>What other stakeholders should be involved?</p>
<p>How is your notice structured and delivered/to whom?</p>	<p>Operational/logistical issues?</p> <p>(e.g., Application Programming Interface (“API”), integration of multiple data sources, possibility/feasibility of connecting to Health Information Exchange (“HIE”))</p>	<p>If working with another party, have you conducted privacy and security due diligence?</p>

HubCo is a technology company with a robust health data platform that performs a variety of functions – e.g., backend hosting of mobile apps, data aggregation, analytics, technology integrations, deidentification, etc. It is used by many companies to facilitate data sharing/exchange (e.g., between providers, payers, health apps, etc.), matching functions across data sets, develop insights, etc. In general, as a condition of using HubCo’s services, HubCo requires data contributors to: (a) allow HubCo to use data to “improve the services”; (b) allow HubCo to create and share deidentified data (and retain such data post-termination of any contractual relationship); and (c) represent that the data contributor has obtained all necessary consents and authorizations for HubCo to perform such functions. Over the years, HubCo has amassed information regarding millions of people.

A life sciences company (LifeCo) wants to develop a patient-facing app to facilitate creation of patient-generated health data, including information about drug adherence, vital signs, etc.

LifeCo plans to use HubCo to: (a) host the app and patient data; and (b) analyze the data to provide to inform development of clinical guidelines.

LifeCo is considering two business models: (a) partnering with HCPs (in which case app would also push data back to the HCP EHR); or (b) direct to consumer.

---

## **Discussion Questions:**

Overarching question: How does analysis change if LifeCo is partnering with HCPs vs. pursuing a “direct-to-consumer” model?

- What laws does this trigger?
  - If HIPAA does not apply, would state equivalents (e.g., CMIA) apply?
  - CCPA vs. CMIA? FTC Section 5?
  - ONC Information Blocking?
- For what purposes can LifeCo use the data under each approach?
  - Can LifeCo use the data to improve/develop the app?
  - Can LifeCo de-identify the data and use it for other purposes?
- Does the analysis change if this is part of a clinical research study?
- Does the individual need to execute any authorization/consent?
- What privacy notice should be presented and by whom?
- What security concerns are there?
- What types of agreements are required and between whom?

## HubCo Use Case # 2

A large health system (“HealthCo”) wants to leverage HubCo to help close care gaps and coordinate care with other providers to improve outcomes and reduce costs. HubCo will work with other providers who also choose to share data for care coordination purposes to connect providers with overlapping patients.

### **Discussion Questions:**

- What agreements are necessary?
  - Between HubCo and HealthCo?
  - Between HealthCo and other providers?
- Does it matter if the data flows through HubCo vs. HubCo facilitating a direct connection between providers/their EHRs via API?
  - Will HubCo become an Health Information Network (“HIN”) under the ONC Information Blocking Rule?
- Are any authorizations needed?
- What privacy notice should be presented and by whom?
  - Are HIPAA Notice of Privacy Practices enough?

HubCo has been approached by a number of third parties offering to pay for access to HubCo's "deidentified" data set.

### **Discussion Questions:**

- What level of "deidentification" is needed based on the "source" of the data?
  - HIPAA deidentification vs. CCPA deidentification
  - How important is it to prohibit recipient from reidentifying the data?
  - What does the contract say?
- What contract is needed with the recipient of the deidentified data set?
  - CCPA AB 713
- State law issues
  - Would HubCo be a data broker?

# QUESTIONS?

---

