
Morgan Lewis
TECHNOLOGY MAY-RATHON
Digital Health Privacy: Focus on AI
May 25, 2021
W. Reece Hirsch, CIPP/US
Lauren Z. Groebe
© 2021 Morgan, Lewis & Bockius LLP

Presenters

W. Reece Hirsch

Lauren Z Groebe

Morgan Lewis

Digital Health Privacy: Focus on AI

- Topics to Be Discussed Today Include:
  - Overview of OCR and the FTC Regulation of Digital Health Privacy
  - Business Associate Status, Consequences and Scenarios
  - AI and Healthcare Privacy: De-identification, Use, Research, and More
  - AI and FTC Privacy Regulation and CCPA Applicability
  - HIPAA and Big Data
  - Key Takeaways

AI Technology is Relatively New, the Healthcare Privacy Laws … Not So Much

- When HIPAA was enacted in 1996, there were no smartphones, no mobile apps, no cloud computing, and no AI/ML (machine learning)
  - HIPAA Privacy Rule: effective April 14, 2003
  - HIPAA Security Rule: effective April 21, 2005
  - HITECH regulations: compliance date September 23, 2013

- One of the themes of digital health privacy law is the effort to apply existing privacy laws to this new landscape of:
  - Healthcare mobile apps
  - Wearable devices
  - Cloud hosting services
  - Artificial intelligence/Machine learning

Privacy by Design

- For companies venturing into the digital health space, privacy and security are critical issues that must be addressed from Day One
  - For startups, questions about privacy and security will be among the first that get asked by customers and potential acquirers
  - The due diligence process will show when a company scrambled to improve privacy and security immediately prior to a potential acquisition
  - For established companies venturing into digital health, a stumble in the digital privacy space can damage a brand and customer relationships
- Privacy by design is the FTC's mantra, banking in privacy and security during the development of a product or service

The FTC and OCR

- One overarching theme in digital health privacy is the overlapping jurisdiction of:
  - The Federal Trade Commission, the US privacy regulator with the broadest purview
  - The Dept. of Health and Human Services Office for Civil Rights (OCR), which enforces HIPAA
  - State Attorneys General
- OCR – regulates HIPAA covered entities
  - Health care providers that engage in standard electronic transactions
  - Health plans
  - Health care clearinghouses
- OCR also regulates business associates

The FTC and OCR (cont'd)

- The FTC regulatory authority with respect to privacy and security is based upon its authority to regulate "unfair or deceptive acts and practices" under Section 5 of the FTC Act
  - An inaccurate or misleading statement or omission in a privacy policy, a user interface, or in other consumer-facing material can constitute a deceptive practice
- In 2005, the FTC used the "unfairness doctrine" in an enforcement action involving BJ's Wholesale Club
  - The unfairness doctrine allows the FTC to take action against businesses for failure to have reasonable data security practices, even in the absence of a deceptive statement on the subject

Consumer-Generated Health Information

- The FTC has taken note of the vast volumes of health information that consumers are sharing through mobile apps, wearable devices, and personal health records, referred to as consumer-generated health information (CHI)
- May 2014: FTC conducts a seminar entitled "Consumer Generated and Controlled Health Data"
- April 2016: FTC, in conjunction with OCR and FDA, releases "Mobile Health Apps Interactive Tool"
- October 2016: FTC and OCR put out business guidance entitled "Sharing Health Information? Look to HIPAA and the FTC Act"
- December 2017: FTC puts out consumer education entitled "DNA Test Kits: Consider the Privacy Implications"
- March 2019: FTC issues guidance for businesses selling genetic testing kits

Early OCR and FTC Privacy Enforcement

April 2017: OCR enters into a no-fault settlement agreement with CardioNet, a wireless cardiac monitoring service provider

- First HIPAA settlement involving a mobile health provider; $2.5M settlement amount
- A laptop was lost containing health information of 1,391 individuals
- Resolution agreement alleged that CardioNet had an insufficient security risk analysis and had not fully implemented its HIPAA Security Rule policies and procedures, which were in draft form

June 2016: FTC enters into a settlement agreement with Practice Fusion, an electronic health record company

- Charged that Practice Fusion misled consumers by soliciting reviews of doctors without disclosing adequately that reviews would be publicly posted, resulting in public disclosure of patients' sensitive personal and medical information

Healthcare Mobile Apps

- In February 2016, OCR released "Health App Use Scenarios & HIPAA"
  - Provides examples of how HIPAA applies to mobile apps that collect, store, manage, organize or transmit health information
  - Six specific scenarios demonstrating when app developers are, and are not, regulated as HIPAA business associates
- July 2020: FTC's PrivacyCon panel on health apps demonstrates the agency's continuing interest in digital health
- September 2020: OCR releases a new resource page for mobile app developers
  - Health App Use Scenarios unchanged
  - New page on "Access Right, Apps, and APIs"

Mobile App Scenario 1

- A consumer downloads a health app to her smartphone
- Populates it with her own health information
- No relationship between the mobile app and the consumer's health care providers or health plan
- Is the app developer subject to HIPAA regulation?
- Is the app developer subject to FTC regulation?

HIPAA Business Associate Definition

- A business associate is
  - A person or entity
  - **Acting on behalf of a covered entity**
  - That creates, receives, ***maintains*** or transmits PHI
  - For a function or activity regulated by HIPAA (a covered entity function)
- "Acting on behalf of" language is key to so many digital health privacy issues
- In mobile app Scenario 1, the app developer is "acting on behalf of" the consumer, not a covered entity
- OCR issued a fact sheet clarifying direct liability of business associates: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html

Mobile App Scenario 2

- A provider contracts with a health app developer for patient management services
  - Remote patient health counseling
  - Monitoring of patients' food and exercise
  - Patient messaging
  - EHR integration
- Provider instructs her patients to download the app to their smartphones
- Is the developer a business associate?
- Does the FTC still have jurisdiction to regulate the developer?

OCR or FTC Regulation? Follow the Money

- Based upon a series of OCR guidance documents, it seems that one test for determining whether an app developer or other digital health company is acting on behalf of the consumer or the covered entity is:
  - Who's paying for the service?
  - If the consumer is your customer, you will probably be subject to FTC regulation, but not HIPAA
  - If the provider is your customer, you will probably be a HIPAA business associate
- In the prior scenario, if the developer also offered a direct-to-consumer version of the same app, that would not be subject to HIPAA

Questions to Ask Regarding Business Associate Status

- OCR's Health App Guidance provides a series of questions that developers should ask to determine if they are business associates:
  - Does the app create, receive, maintain or transmit identifiable health information?
  - Is the health app selected independently by the consumer?
  - Are all decisions to transmit health data to third parties controlled by the consumer?
  - Does the developer have any contractual or other relationships with covered entities besides interoperability agreements?

The Consequences of BA Status

- Whether or not a developer is a business associate may have a significant impact on the developer's information collection and disclosure practices
  - If a BA, then BA is acting on behalf of the health care provider or health plan and is governed by rigorous HIPAA privacy rules
    - With limited exceptions, the developer can use and disclose PHI only to provide the contracted services to the covered entity
  - If not a BA, then developer will be covered by the FTC's Section 5 enforcement authority
    - Developer has latitude to use and disclose personal information collected through the app so long as it is not misleading consumers or causing substantial injury to consumers in ways that are more harmful than helpful to consumers or the marketplace overall

Bifurcated BA Status?

- For an app developer that has both HIPAA business associate and consumer-directed operations, it may be necessary to segregate personal information collected through the two channels
  - Different privacy rules apply
  - Also different security rules
    - Although the HIPAA Security Rule is generally viewed as representing a reasonable, flexible data security standard
- Although HIPAA's "hybrid entity" concept applies only to covered entities, is it reasonable to assume that a similar approach could be applied to business associate entities with BA and non-BA functions?
- Do the HIPAA Security Rule and the FTC's "unfairness doctrine" under Section 5 of the FTC Act reflect consistent visions of what constitutes appropriate data security?

AI and Healthcare Privacy

- Artificial intelligence (AI) offers potential for improving healthcare but also potential privacy challenges
- Key questions to consider:
  - Is it possible for the AI developer to use de-identified data?
  - Is AI processing a "use" of PHI under HIPAA?
  - Is AI Processing a Permitted Purpose Under HIPAA?
  - Is Development of AI a Research Activity?

AI and Healthcare Privacy: De-identification

- Developing AI requires access to vast amounts of health information in order to teach AI the vocabulary and grammar of medicine and structure and meaning of electronic health record (EHR) and claims data
- Use of de-identified PHI (if feasible) reduces obstacles because it is not subject to HIPAA use and disclosure limitations, "minimum necessary" standard or prohibition on sale
- Two permitted methods of de-identification: (1) "Safe harbor" method removes 18 categories of identifiers and cannot have actual knowledge that remaining information can identify an individual and (2) "Expert determination" method, determination that risk of identifying individual is "very small"
- For unstructured data it may be difficult to ensure all 18 identifiers are removed

Is AI Processing a "Use" of PHI?

- December 2000 commentary to proposed HIPAA Privacy Rule:
  - "We interpret 'use' to mean only the uses of the product of the computer processing, not the internal computer processing that generates the product."
- The world has changed a great deal since 2000, and it's not clear that this interpretation would hold today
- HHS 2019 guidance on ransomware provides that access and encryption of data by a third party's malware constitutes a "disclosure"
- Is there a distinction between a search query that identifies specific data, as opposed to AI's broad use of data to "learn"?
- If PHI is not de-identified, then this question of what constitutes a use is critical

Is AI Processing a Permitted Purpose Under HIPAA?

- If AI processing is a "use" and involves PHI that hasn't been de-identified, then it may be a permitted activity under HIPAA:
  - Treatment: Must involve a health care provider and a single individual
  - Payment: May include using AI to identify billed services that may be medically unnecessary
  - Health care operations: AI could be used to conduct many of the activities that qualify, including "population-based activities relating to improving health or reducing health care costs"
    - Quality assessment and improvement
    - Case management and care coordination
    - Fraud and abuse detection

Is Development of AI a Research Activity?

- Development of AI could qualify as a "health care operations" use if it relates to population-based activities or "protocol development"
- However, if the AI activity constitutes "research," then one of the following may be required:
  - HIPAA authorization signed by the patient
  - IRB waiver of authorization
  - Use of limited data set and entering into data use agreement with AI developer
- "Research" is defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to ***generalizable knowledge***"
  - HHS has stated in commentary that the "primary purpose" of the activity will govern

AI Processing By HIPAA Business Associates

- If AI processing is a permitted treatment, payment, or health care operations activity of a HIPAA covered entity
  - Then the covered entity may contract with a business associate to perform that function
- Does business associate have an independent right to conduct AI processing of PHI?
  - If BA has the right to de-identify, then the BA may use that de-identified data for AI
  - BA is also permitted to use PHI for "the proper management and administration of the business associate"
  - BA may use PHI to provide "data aggregation" services to multiple covered entities if expressly permitted by the business associate agreement

AI and FTC Privacy Regulation

- April 8, 2020 blog post by Andrew Smith, Director, FTC Bureau of Consumer Protection
  - "Using Artificial Intelligence and Algorithms"
- Guidance includes:
  - Don't deceive consumers about how you use automated tools
  - Be transparent when collecting sensitive data
  - If you deny consumers something based on algorithmic decision-making, explain why
  - Make sure your AI models are validated and revalidated to ensure that they work as intended, and do not illegally discriminate
  - Protect your algorithm from unauthorized use
  - Consider your accountability mechanism (use of independent standards or independent experts)

AI and the California Consumer Privacy Act

- CCPA defines "personal information" to include:
  - "Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes"
- When a California consumer exercises the "right to know," a business may be required to disclose this profiling data, including when it was developed using AI
- CCPA privacy notices must identify the business or commercial purpose for collecting or selling personal information
  - Would include being transparent about use of data for AI development purposes
- CCPA will often apply to digital health businesses that are under FTC jurisdiction

AI and CCPA's Right to Know

- How far should a business go in its CCPA privacy policy to notify consumers regarding
  - How personal information is used to train specific AI/ML models?
  - "Explainable" vs. "Black box" AI

- Explainable AI may be particularly critical for healthcare applications
  - Example: Physician uses AI analytics to detect cancerous lesions
    - Virtual assistant may explain how each variable in an MRI image is analyzed and taken into account in considering the probability of cancer

AI and CCPA's Right of Deletion

- If an AI/ML model was trained with user data, CCPA would require removal of the data in the training dataset wherever it is stored when the right of deletion is exercised
  - This means tracking the lineage of data being used in model training
- If an individual user can be identified from a model's recommendation, is it necessary to delete the model itself, in addition to deleting underlying user data?
- Deleting the AI/ML model may not be feasible in response to each user's request for deletion
  - Alternatively, could identify the impact of the user data in model generation using explainability techniques
  - Then regenerate a new model only if the impact of the data subject's deletion was sizable (e.g., more than 1%)

Big Data and Covered Entities

- For health plans, pharmacies and other HIPAA covered entities (CEs) that maintain large databases of medical information, big data analytics are typically permitted with respect to their own members/patients

- Big data analysis can usually fit within a covered entity's permitted uses of protected health information (PHI) for its "health care operations" activities

  – Sometimes "treatment" or "payment"

3 Rules for BAs and Big Data

- Management and administration
- Data aggregation services
- De-identification

Management and Administration (Use)

- Pursuant to the terms of a Business Associate Agreement (BAA), a business associate (BA) is prohibited from using or disclosing a CE's PHI other than as permitted or required by the BAA or as required by law

- BAA may permit the BA to **use** the information received by the BA, if necessary "[f]or the proper management and administration of the business associate …"

Management and Administration (Disclosure)

- BAA may also permit a BA to **disclose** PHI for its management and administration purposes if:
  - The disclosure is required by law OR
  - The BA obtains reasonable assurance from the person to whom the PHI is disclosed that it will be held confidentially or used or further disclosed only as required by law or for the purpose for which it was disclosed AND
  - The person notifies the BA if the confidentiality of the PHI is breached

What Is Management and Administration?

- Common provision in BAAs
  - Without it, BA might not be permitted to use PHI for many activities vital to its business
  - "Management" and "administration" are not defined in the HIPAA regulations or commentary
- However, in 2000 commentary to the HIPAA Privacy Rule, OCR did offer this interesting comment:

HHS Comment on Data Mining

- "Aside from disclosures for data aggregation and **business associate management**, the business associate contract cannot authorize any uses or disclosure that the covered entity itself cannot make. Therefore, ***data mining*** by the business associate for any purpose not specified in the contract is a violation of the contract and grounds for termination of the contract by the covered entity."

- Indicates that data mining/big data analytics may be conducted by a BA, but only if provided for in the agreement.

HHS Comment on Data Mining (cont.)

- HHS's commentary could also be read to suggest that a BA is prohibited from using PHI for the BA's commercial purposes unrelated to the services that a CE has contracted for and not expressly authorized by the BAA, such as data mining

- Some activities of a BA may be reasonably characterized as "management and administration" activities, such as --

"Safe Zone" Management and Administration Functions

- Quality assurance
- Utilization review
- Compliance
- Fraud prevention
- Auditing
- Cost-management and planning-related analyses
- CEs are permitted to engage in these sorts of types of activities as part of permitted "health care operations"

Management and Administration as "Back-Office Functions"

- It seems reasonable to say that these "safe zone" functions are integral to a BA's current and future suite of products and services
  - They could also be characterized as essential "back office" functions
- But what if effective management of a BA's business ***requires*** data mining/big data analytics?
- Businesses are increasingly data-driven
  - Data analytics is often critical to evolving existing products and services and developing new ones

Data Analytics as Management and Administration

- What if data analytics is necessary to develop a new protocol to identity plan members that are at risk for diabetes?

- Is crawling and mapping customer data necessary to facilitate development of future products or services or research and development?

- In the absence of interpretive guidance from OCR, we must rely on the plain meaning of the terms "management" and "administration"

Data Aggregation

- "Data aggregation" is defined as a BA's combining of PHI received from multiple CEs to permit data analyses that relate to the "health care operations" of the respective covered entities

- Like "management and administration," this is an optional provision in BAAs

- HHS states that the data aggregation rule clarifies the ability of CEs to contract with BAs to undertake quality assurance and comparative analysis that involve the PHI of more than one contracting CE

"Health Care Operations" Defined

- "Health care operations" is defined to include a wide range of covered entity business functions, including:
  - "population-based activities relating to improving health or reducing health care costs"

- Data aggregation services rules can be very useful in supporting the population-based health objectives of many big data projects

Data Aggregation Requirements

- BA must enter into BAAs that permit data aggregation services
- All of the PHI analyzed/utilized by the BA as part of its data aggregation service is received by the BA in its capacity as a BA of a CE
- The BA's customers receiving the product of data aggregation services are CE's for which the BA is acting as a BA
- The data aggregation services relate to one of the types of activities listed in the definition of "health care operations"

Limited Uses of Aggregated Data

- Important to remember that data analysis resulting from data aggregation may only be shared with CEs that shared PHI with the BA

- However, if the BA also has permission to de-identify PHI in its BAA, then the analysis performed through data aggregation may satisfy HIPAA's de-identification standard

- If PHI is de-identified, then it is no longer regulated under HIPAA and may be shared with any third parties

Takeaways

- Navigating this new digital health privacy landscape requires
  - Keeping an eye on the latest enforcement actions by OCR, FT,C and state Attorneys General
  - Reviewing the latest guidance documents interpreting laws and regulations like HIPAA and Section 5 of the FTC Act
  - Incorporating emerging privacy and security best practices, including Privacy by Design and Security by Design
  - Law of AI privacy remains unsettled
- Remember that many digital health companies straddle multiple privacy and security regulatory regimes
- KNOW WHEN YOU'RE CROSSING ONE OF THOSE LINES!

Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

Morgan Lewis

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at **www.morganlewis.com/topics/coronavirus-covid-19**

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to **subscribe** using the purple "Stay Up to Date" button.

W. REECE HIRSCH

W. Reece Hirsch
San Francisco
+1.415.442.1422
reece.hirsch@morganlewis.com

W. Reece Hirsch co-heads the firm's privacy and cybersecurity practice and counsels clients on a wide range of US privacy issues, specializing in healthcare privacy and digital health. Reece counsels clients on development of privacy policies, procedures and compliance programs, security incident planning and response, and online, mobile app, and Internet of Things privacy. Reece counsels clients in healthcare privacy and security matters, such as compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, state medical privacy laws, and Federal Trade Commission standards applicable to digital health companies. He has represented clients from all sectors of the healthcare industry on privacy and security compliance, including health plans, insurers, hospitals, physician organizations, and healthcare information technology, digital health, pharmaceutical, and biotech companies. Reece also advises clients on privacy issues raised by the coronavirus (COVID-19) pandemic, including those relating to workplace testing, HIPAA waivers and enforcement discretion, contact tracing, telehealth, and work-from-home and return-to-work policies.

LAUREN Z GROEBE

Lauren Z Groebe
Chicago
+1.312.324.1478
lauren.groebe@morganlewis.com

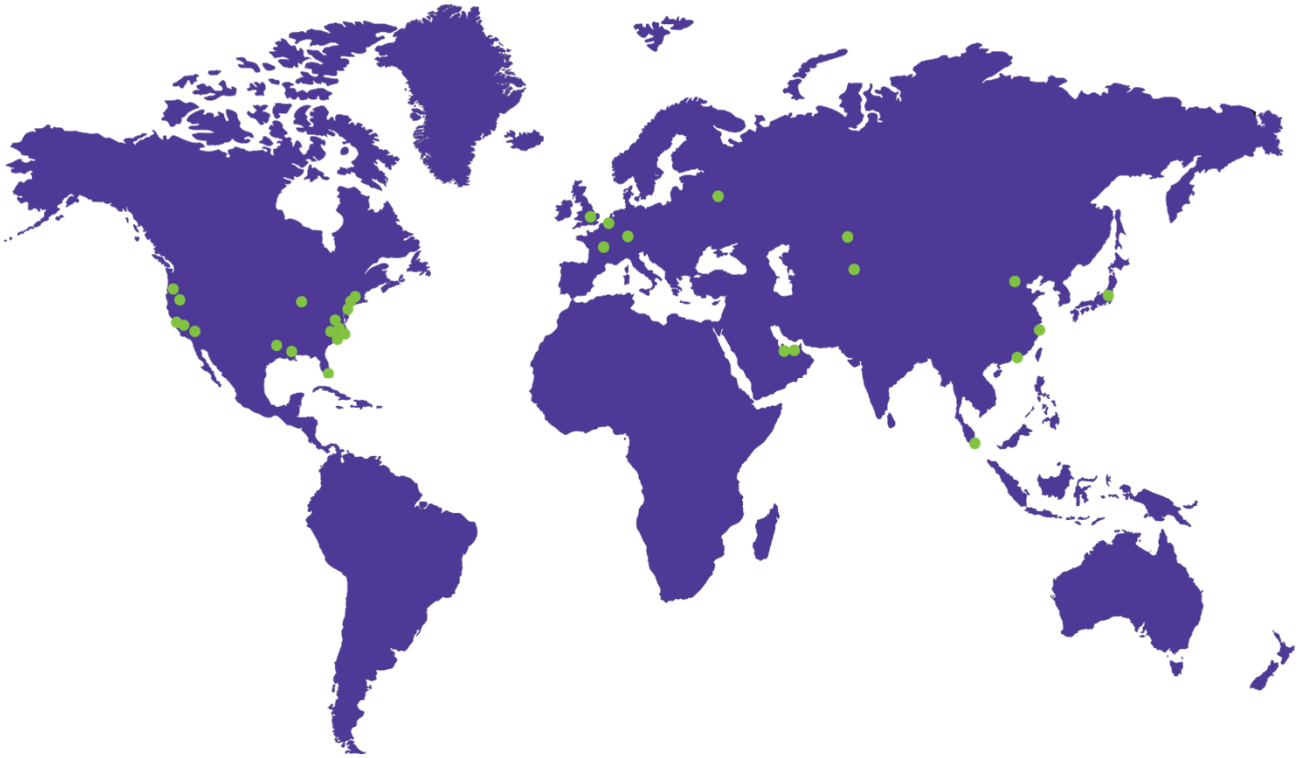
Lauren Z Groebe focuses her practice on regulatory and transactional matters affecting clients in the healthcare sector. She counsels hospitals, health systems, hospices, pharmacies, and private equity clients, among others, across a range of regulatory issues, including matters related to compliance with HIPAA, the 340B Program, the Sunshine Act, fraud and abuse laws, Medicare and Medicaid enrollment, and licensure requirements. Lauren also advises clients on the corporate and healthcare regulatory aspects of merger and acquisition transactions.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU