
Morgan Lewis
PRIVACY + SECURITY FORUM
DIGITAL HEALTH PRIVACY:
THERE'S AN APP FOR THAT
October 6, 2017
© 2017 Morgan, Lewis & Bockius LLP

A Note on Format

- The content of these slides was developed solely by Morgan Lewis, and does not reflect the comments or opinions of OCR or FTC
  - Offered as a basis for comment and response by the panelists
- Presenter: Reece Hirsch, co-head of Privacy & Cybersecurity Practice, Morgan Lewis

- Panelists:
- Cora Tung Han, Senior Attorney, Federal Trade Commission
- Deven McGraw, Deputy Director for Health Information Privacy, HHS Office for Civil Rights

The Technologies are New, The Laws … Not So Much

- When the Health Insurance Portability and Accountability Act was enacted in 1996, there were no smart phones, no mobile apps, no cloud computing
  - HIPAA Privacy Rule became effective April 14, 2003
  - HIPAA Security Rule became effective April 21, 2005
  - Compliance date of HIPAA Final Rule: September 23, 2013
- In recent years regulators and digital health companies have had to interpret existing laws to fit this new landscape of
  - Healthcare mobile apps
  - Wearable devices
  - Cloud hosting services
  - Personal health records

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 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, baking 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 U.S. 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
  - 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 in a privacy policy can constitute a deceptive practice
- In 2005, 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
- Often referred to as consumer-generated health information (CHI)
- May 2014: FTC conducts a seminar entitled "Consumer Generated and Controlled Health Data"
- Former FTC Commissioner Julie Brill made clear that she considered CHI sensitive and in need of greater protections than other types of consumer data
- April 2016: FTC puts out business guidance entitled "Mobile Health App Developers: FTC Best Practices"
- FTC's February 2013 staff report "Mobile Privacy Disclosures: Building Trust Through Transparency" offers important, but non-healthcare-specific guidance

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
  - Issued on OCR's mHealth Developer Portal, which provides guidance and responds to questions from app developers regarding HIPAA
  - Six specific scenarios demonstrating when app developers are, and are not, regulated as HIPAA business associates

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

Mobile App Scenario 2

- Consumer downloads a health app to her smartphone to help manage a chronic condition
- App developer and healthcare provider have entered into an interoperability arrangement at consumer's request to facilitate secure exchange of health information
- Consumer inputs information on the app and directs it to transmit the information to the provider's EHR
- Consumer accesses provider's test results through the app
- Is the app developer a HIPAA business associate?
- What if the app's privacy policy is not posted in the app store where the app is downloaded and is not conspicuously available to the consumer?
- When the consumer is about to send health information from the app to the provider's EHR, should there be some form of "just in time" notification?

Mobile App Scenario 3

- A provider contracts with a health app developer for patient management services
  - Remote patient health counseling
  - Monitoring 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 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 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 third-party entities besides interoperability agreements?

Close Questions/Gray Areas

- But what if the provider is paying for only a portion of the app?
  - Paying 75% of the fee for the app?
    - And offering members only one choice of app?
  - Providing a smart phone or tablet to be used to download the app?

Close Questions/Gray Areas

- What if the app developer provides a 25% discount on the app to a particular health plan's members?
  - What if the discount is offered across the board to members of all national health plans?

Close Questions/Gray Areas

- What if the provider is only paying 25% of the cost of the app?
  - Offering a coupon or rebate for a portion of the cost of a device used with an app?

The Consequences of BA Status

- Whether or not a developer is a business associate will have an enormous 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 is regulated by the FTC and will be governed by the mobile app's posted privacy policy
    - Developer has great latitude to use and disclose personal information collected through the app so long as there is disclosure and appropriate consent obtained through the privacy policy
    - Transparency is key

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 applicable to business associates is generally viewed as representing a reasonable, flexible data security standard

Parallel Security Standards

- 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?

OCR's First Mobile Health Privacy Enforcement Action

- April 24, 2017: OCR enters into a no-fault settlement agreement with CardioNet, a wireless cardiac monitoring service provider
  - The first HIPAA settlement involving a mobile health provider
  - $2.5 million settlement amount
  - Corrective action plan
- Arose out of incident in which 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

FTC Mobile Health App Tool

- FTC, OCR and FDA developed a "Mobile Health Apps Interactive Tool"
  - Provides a list of questions that can help an app developer determine whether it is subject to:
    - HIPAA
    - FTC Act
    - FTC's Health Breach Notification Rule
    - Federal Food, Drug and Cosmetic Act
      - Is your app intended for use in the diagnosis of disease or other conditions?
      - Is your app a "mobile medical device," such as an accessory to a regulated medical device?
      - Does your app pose "minimal risk" to a user?

Geofencing

- April 2017: Massachusetts Attorney General enters into a no-fault settlement with a digital advertising company, Copley Advertising
  - AG alleged that Copley set virtual fences – a practice known as "geofencing" – around reproductive health clinics and methadone clinics in several states
  - When GPS data showed that individual was near a reproductive health clinic, an ad about alternatives to abortion would be triggered
  - Geofencing technology enables "tagging" of smartphones and other mobile devices as they enter or leave a certain area
    - Causes targeted third-party ads to display once a mobile app or web browser is opened by the consumer

Geofencing (cont.)

- How might the FTC evaluate the practice of geofencing?
- If the digital advertising company was a business associate delivering targeted ads on behalf of a HIPAA covered entity health care provider, how might OCR view geofencing?

Activity Trackers and Wearable Devices

- Proliferation of activity trackers and other sensor-based wearables raises many of the same privacy regulatory issues as health mobile apps
- Activity trackers are often sold directly to the consumer
  - In those cases, the company would not be a HIPAA business associate because it is acting on behalf of the consumer, not on behalf of a covered entity
- But if a health plan enters into an arrangement to purchase activity trackers for its members, that may trigger a BA relationship
  - Still a facts and circumstances test: How much is the health plan paying? How much control does the plan member have over the choice of the device and sharing information with the plan?

Employer vs. Employer Group Health Plan

- If an activity tracker is sold to an employer (in its capacity as an employer) to make the devices available to its workforce
  - Probably NOT a business associate relationship
  - An employer, acting in its capacity as an employer, is not a HIPAA covered entity and the medical information they hold is not PHI
- HOWEVER, if the activity trackers are sold to the employer's group health plan (which is separate and legally distinct from the employer/plan sponsor)
  - Then the activity tracker company probably would be a business associate
  - Employer group health plans are almost always health plan covered entities under HIPAA

The Internet of Things

- In 2013, the number of mobile devices connected to the Internet became greater than the number of people in the world
- Number of devices connected to the Internet worldwide is estimated to reach more than 20 billion by 2020
- Many of these devices, such as activity trackers and smart medical devices, collect CHI
- How do you implement reasonable privacy and security for this enormous proliferation of connected devices?
- October 2016: IoT devices such as digital cameras and DVR players were you used in a distributed denial of service attack that shut down major websites like Twitter, Netflix and CNN

FTC Intends to Police IoT

- May 2015: Former FTC Commissioner Julie Brill declares that the FTC's enforcement powers extend to cover privacy and security risks posed by the IoT
  - No specific privacy law that directly targets IoT data collection and security
  - FTC regulates IoT based on jurisdiction over unfair and deceptive trade practices under Section 5 of the FTC Act
- Section 5 doesn't specifically address application of privacy principles to cutting-edge technologies
  - Concepts of deception and unfairness may be interpreted to cause companies to examine
    - What they are telling consumers about data collection and use
    - What consumers understand about those practices
    - What are their data security practices

Adapting Privacy Best Practices to Connected Devices

- Privacy regulation is based on traditional notions of "notice" and "consent"
  - But those concepts must be adapted to apply to IoT
- Wearable fitness trackers typically don't have a user interface to serve as a means to present consumers with choices about data collection
- Connected devices may become too numerous for consumers to effectively manage their information
- Brill urged companies to "get creative" about providing privacy transparency and control for consumers to manage their data
  - Example: "Command center" that runs multiple household devices and can describe in simple terms how information is being collected and used across those devices

The FTC Weighs In

- In January 2015, the FTC issued the report "Internet of Things: Privacy & Security in a Connected World"
  - Based on input from technologists, academics, industry representatives, consumer advocates at November 2013 FTC workshop in D.C.
  - Report is limited to IoT devices that are sold to or used by consumers
  - Recommended practices document, does not have the force of law or regulations
  - But may provide insight into future FTC enforcement actions

Hypothetical: Smart Glucose Meter

- Manufacturer of a smart glucose meter that stores consumer's glucose level information in the cloud
- If manufacturer sells the meter directly to the consumer, how is the manufacturer regulated?
- Presentation of privacy policy
  - What if the manufacturer includes its privacy policy only on its corporate website?
  - What if the consumer clicks acceptance of a privacy policy when she accesses data in the cloud?
- If manufacturer sells smart glucose meters to a medical practice, which then offers them to patients, how is the manufacturer regulated?
  - See OCR cloud computing guidance

Personal Health Records

- What is a Personal Health Record (PHR)?
- No universal definition
- Generally, an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in his or her own care
- Mobile health apps and some IoT devices can take on characteristics of a PHR depending upon amount and type of CHI collected
- Distinct from an electronic medical record (EMR), which is maintained and largely controlled by a health care provider

HIPAA and PHRs

- OCR issued guidance document "Personal Health Records and the HIPAA Privacy Rule"
- Earlier statement of many of the principles elaborated upon in mobile health app and cloud computing guidance
- Consumer-directed PHRs not offered by HIPAA covered entities are not subject to HIPAA regulation
- The fact that a consumer places copies of their medical records in a PHR does not create a business associate relationship
- PHR vendor must be "acting on behalf of" a HIPAA covered entity to be a business associate

Hypothetical: Health Plan PHR

- A health plan offers a PHR for its plan members so that they can better manage their health
  - Uses the PHI to facilitate granting HIPAA rights to access and amend PHI, obtain an accounting of PHI disclosures, and receive a Notice of Privacy Practices
  - How will the health plan's PHR be regulated?

Hypothetical: Direct-to-Consumer PHR

- PHR company offers a similar PHR directly to consumers
- Plan member can exercise right to access health plan's PHI and place that copy in their PHR
- PHR requires users to agree to its privacy policy at account creation
- PHR company claims in its advertising to be "HIPAA compliant"
- PHR company claims to have voluntarily implemented HIPAA Security Rule standards

FTC's Health Breach Notification Rule

- Recognizing the limits of HIPAA's statutory reach, the FTC issued a Health Breach Notification Rule in 2009
  - Mirrors the HIPAA Breach Notification Rule
- Applies to:
  - A vendor of PHRs
  - A PHR-related entity
  - A third-party service provider for a vendor of PHRs or a PHR-related entity
- These entities must notify their customers and others if there's a breach of unsecured, individually identifiable health information

Vendor of Personal Health Records Defined

- A business is a vendor of personal health records if it "offers or maintains a personal health record"
- A PHR is defined as an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and is managed, shared, and controlled by or primarily for the individual"
- Could the FTC Breach Notification Rule apply to mobile apps and wearable devices that have some characteristics of a PHR?

Virtual Assistants and Healthcare

- Do voice-activated virtual assistants like Amazon's Alexa and Google Assistant represent the next wave of digital health innovation?
- Health systems are beginning to experiment with virtual assistants to keep patients informed and engaged
- Alexa currently offers:
  - Medical information
  - "Medical advice" from a "physician A.I."
  - Tool that lets diabetes patients track their blood sugar information by telling it to Alexa
- Potential HIPAA and FTC Act Section 5 issues?

What's to Come?

- What is the outlook of OCR and FTC with respect to the digital health privacy space?
- Guidance documents in the pipeline?
- Areas of likely enforcement or concern?

Takeaways

- Navigating this new digital health privacy landscape requires
  - Keeping an eye on the latest enforcement actions by OCR, FTC 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
- Remember that many digital health companies straddle multiple privacy and security regulatory regimes
- KNOW WHEN YOU'RE CROSSING ONE OF THOSE LINES!