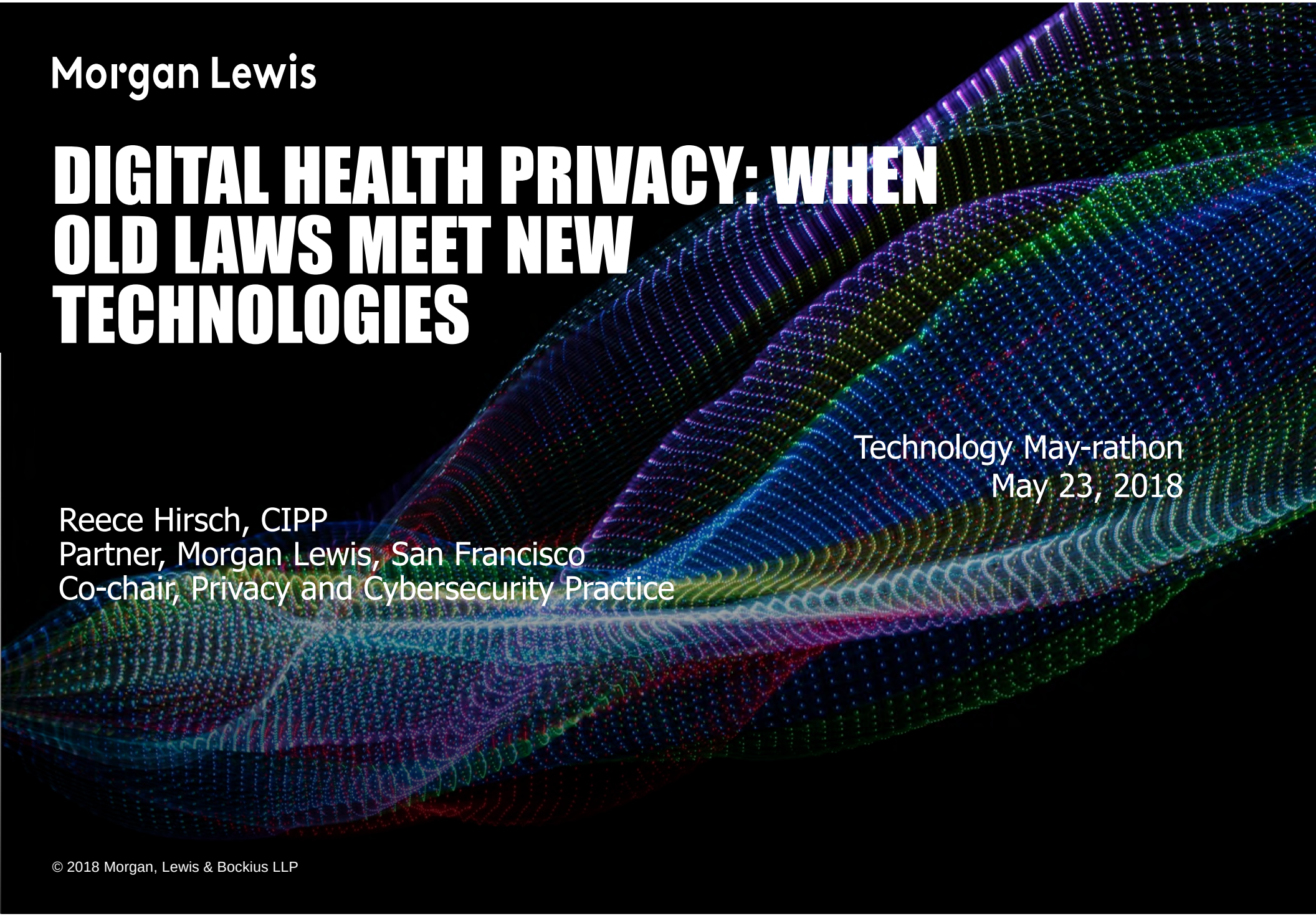


Morgan Lewis

DIGITAL HEALTH PRIVACY: WHEN OLD LAWS MEET NEW TECHNOLOGIES

Technology May-rathon
May 23, 2018

Reece Hirsch, CIPP
Partner, Morgan Lewis, San Francisco
Co-chair, Privacy and Cybersecurity Practice

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, and 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 stretch, tweak, and 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 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
  - Healthcare providers that engage in standard electronic transactions
  - Health plans
  - Healthcare 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, 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
- 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 titled "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

- 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 healthcare providers or health plan
- Is the app developer subject to HIPAA regulation?
- NO: The developer is not acting as a HIPAA covered entity (not a health care provider or health plan)
  - Also not a HIPAA business associate because no covered entity is involved

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?

Mobile App Scenario 2: NOT a Business Associate

- NO – the app developer is not a business associate
- Developer is not creating, maintaining, or transmitting PHI on behalf of a covered entity
- Developer is still acting on behalf of the consumer
- Interoperability arrangement doesn't create business associate relationship because it is intended to facilitate access to health information initiated by the consumer

Mobile App Scenario 3

- 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 his patients to download the app to their smartphones
- Is the developer a business associate? YES
  - Provider is contracting with developer for a service that involves creating, receiving, maintaining, or transmitting PHI

Who Is A Business Associate? Follow the Money

- In a series of OCR guidance documents, it's become clear that one of the best litmus tests 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 app, that would not be subject to HIPAA

Close Questions

- But what if the provider is paying for only a portion of the app?
  - Paying 75% of the fee for the app?
  - Providing a smartphone or tablet to be used to download the app?
  - Developer is probably a business associate
- 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?
  - OCR guidance doesn't address these questions
- 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?

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?

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 healthcare 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
    - Would likely (but not necessarily) be viewed as consistent with the security standards articulated by the FTC in enforcement actions under the unfairness doctrine
    - Applying HIPAA's hybrid entity concept to business associates

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

The Role of State AGs

- The Copley geofencing settlement demonstrates that the FTC is not the only general privacy regulator
  - State AGs have similar authority to regulate unfair and deceptive practices under the so-called "Baby FTC Acts"
- Analysis of the Copley situation would have been quite different if Copley had been operating as a HIPAA business associate
  - HIPAA imposes strict rules that limit the ability of a covered entity or business to use PHI for marketing purposes
  - State AGs have had authority to enforce HIPAA since enactment of the HITECH Act in 2009

Illinois AG Investigation of Health Websites

- July 2013: Illinois AG Lisa Madigan requested information from eight health-related websites
  - Information about the sites' collection of CHI
  - How CHI is used and shared
  - Percentage of users who click through to read each website's privacy policy
    - Concern that privacy disclosures are often buried in privacy policies not found on websites main pages

New York AG Enters the Fray

- March 2017: New York AG Eric Schneiderman announces settlements with three health app developers for "misleading claims and irresponsible privacy practices" that violated NY consumer protection laws
- Settlements required companies to amend their marketing claims, modify privacy policies, consent to monitoring and pay fines ranging from $5,000-$20,000
- Each of the apps were referred to as "health measurement apps" that purported to measure vital signs, like a traditional medical device, without the assistance of any external device
- "My Baby's Beat," baby heart monitor app that claimed it allowed a pregnant user to monitor her fetus's heartbeat by holding her smartphone to her stomach with the app open

New York AG Enters the Fray (cont.)

- Each of the three health app developers made marketing claims comparing their apps to traditional medical devices
  - Even though apps were not submitted to the FDA
- Health app developers should ensure that any marketing claims are fully supported by data
- If your app has not been submitted to the FDA, do not compare it to an FDA-regulated device
- AG found app privacy policies to be inadequate
  - Presuming consent to policy through use of app
  - Collecting geolocation data without disclosing that fact
  - Stating that GPS could be turned off, but not providing the option

Activity Trackers and Wearable Devices

- Proliferation of activity and fitness 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 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 user interfaces 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, and consumer advocates at November 2013 FTC workshop in DC
  - 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

Example: 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, it's not a business associate subject to HIPAA
- Governed by FTC privacy standards
  - How are privacy practices disclosed to the consumer?
  - When consumers access their data in the cloud, they click acceptance of a privacy policy
- If manufacturer sells smart glucose meters to a medical practice, which then offers them to patients, then it's probably a business associate subject to HIPAA
  - OCR cloud computing guidance would apply

Navigating the IoT

- For companies venturing into the IoT landscape, it's important to remember that:
  - Legal standards are rapidly evolving and still unsettled
  - For that reason, Privacy by Design and Security by Design should be part of the product development process for all IoT devices
  - Those concepts should be revisited regularly as part of a robust privacy and security compliance program

HIPAA and Cloud Computing

- OCR issued 2016 guidance document on cloud computing and HIPAA, recognizing proliferation of
  - Cloud-based electronic medical records
  - Cloud services offering access to networks, servers, storage and applications
- Prior to the HIPAA Final Rule's 2013 compliance date, cloud service providers (CSPs) were not business associates if they did not access, use or disclose PHI
- Business associate definition was modified to include "maintaining" PHI as a basis for a BA relationship

Encrypted Data is PHI, Too

- CSP hosts a hospital's EMR
- All PHI is encrypted and the CSP does not have an encryption key
- Termed "no-view services" by OCR
- While encryption significantly reduces the risk of information being viewed by unauthorized persons, it doesn't alone satisfy HIPAA Security Rule standards
- Risks remain, such as:
  - Corruption of data by malware
  - Risks to physical security (facilities)
  - Recovery of data in emergency or disaster situations

No-View Services

- When a CSP is providing no-view services, OCR acknowledges that it may be appropriate for the covered entity and the business associate to share Security Rule responsibilities
- If the covered entity controls who can view PHI, then it may take responsibility for access controls, like authentication or unique user identification
  - Encryption may be a more appropriate function for the CSP
- The parties can divvy up security responsibilities based upon their respective security risk management plans
  - Along with security risk analysis, the cornerstone of HIPAA Security Rule compliance

No-View Services (cont.)

- Even when the covered entity customer controls authenticating access to ePHI, the CSP may be responsible for
  - Internal controls governing authorized access to the administrative tools that manage the resources
    - Such as storage memory, network interfaces, and central processing units
- Contracts for cloud services can allocate responsibility for compliance with various Security Rule standards
  - OCR says it will take that sort of allocation into consideration in an enforcement action
  - Parties often fail to take advantage of this nuanced approach to BAA contracting

CSPs and Offshoring

- A covered entity or business associate may use a CSP that stores ePHI on servers outside the US if applicable HIPAA requirements are satisfied
- However, if ePHI is being maintained in a country where there are documented increased attempts at hacking or other malware attacks
  - Those risks should be taken into account in the entity's risk analysis and risk management processes
  - Once again, this reflects a degree of nuance that isn't found in many HIPAA risk analyses
- CSPs are generally not "conduits" exempt from business associate rules

So What's a Conduit?

- In commentary to the HIPAA regulations, OCR created the conduit exception
  - A transmission-only service for PHI is not a business associate
  - Applies to paper transmission (couriers and the post office)
  - Applies to electronic transmission (certain telecommunications providers, and messaging services)
  - Temporary storage of PHI incident to transmission is permitted
  - Any access to PHI by a conduit is "random and infrequent" and "transient in nature"
  - Transmission must be the *only* service that the company is providing to the covered entity

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 the 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 that are 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

Example: Health Plan PHR

- A health plan offers a PHR for its plan members so that they can better manage their health
  - HIPAA grants individuals rights to access and amend their PHI, obtain an accounting of PHI disclosures, and receive a Notice of Privacy Practices
  - A PHR can be a means of more effectively providing those rights
  - But the health plan PHR must still abide by HIPAA Privacy Rule limitations on uses and disclosures
  - Health plan PHR must also implement HIPAA Security Rule safeguards

Example: 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 medical information it's not subject to HIPAA Privacy Rule
- Privacy obligations governed by the PHR's posted privacy policy
- Be wary of PHRs (or other products) that advertise themselves as being "HIPAA compliant"
  - A covered entity or business associate can be HIPAA compliant, but not a product or service
- Although not legally required, HIPAA Security Rule represents a good voluntary security standard

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"
- That definition could potentially apply to a wide range of mobile health apps, IoT devices, and other digital health services
- Requirements of the FTC Health Breach Notification Rule are much more detailed and prescriptive than state breach notification laws that would otherwise apply

PHR-Related Entity Defined

- A PHR-related entity
  - Interacts with a PHR vendor either by
  - Offering products or services through the vendor's website (even if the site is covered by HIPAA)
  - Or by accessing information in a PHR or sending information to a PHR
- Example: You have an app that lets consumers upload readings from a device like a blood pressure cuff into a PHR
  - You are a PHR-related entity
  - If you just provide the readings and the individual inputs them into a PHR, you are not a PHR-related entity

FTC Breach Notification Requirements

- Very similar to HIPAA Breach Notification Rule
- If breach involves information of more than 500 people, you must notify the FTC as soon as possible and within 10 business days after discovering the breach
- If the breach involves information of fewer than 500 people, you can send the notice on an annual basis within 60 days of the end of the calendar year
- If the breach involves more than 500 residents of a particular state, you must notify prominent media outlets serving the relevant locale

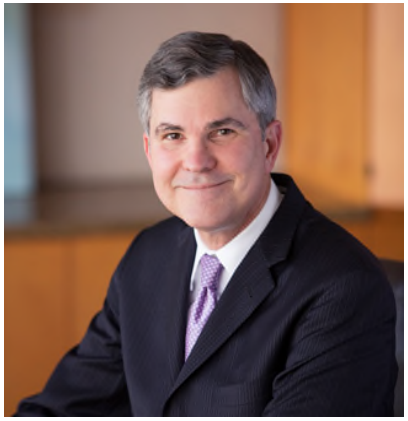
Virtual Assistants and Healthcare

- 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?

Takeaways

- Navigating this new landscape requires
  - Keeping an eye on the latest enforcement actions
  - Reviewing the latest guidance documents for interpreting laws and regulations like HIPAA and Section 5 of the FTC Act
  - Incorporating emerging privacy and security best practices
- Remember that many digital health companies straddle multiple privacy and security regulatory regimes
- KNOW WHEN YOU'RE CROSSING ONE OF THOSE LINES!

Questions



Reece Hirsch

San Francisco, California
tel. +1.415.442.1422
fax. +1.415.442.1001
reece.hirsch@morganlewis.com

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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

Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.