Presenters

W. Reece Hirsch

Partner, FDA & Healthcare

Co-head of Privacy & Cybersecurity Practice

Sydney Reed Swanson

Associate, FDA & Healthcare

Morgan Lewis

A Year of Growth for Digital Health

A number of factors have come together to accelerate the evolution of digital health during the past year

- **COVID pandemic led to significantly increased use of telehealth**
- **Implementation of the CMS and ONC interoperability rules are facilitating patient access to PHI**
- **Publication of proposed modifications to the HIPAA Privacy Rule, with a focus on patient access to PHI**
- **Continued proliferation of digital health mobile apps, wearables and Internet of Medical Things (IoMT) devices**

This presentation will review the latest developments in FTC and OCR enforcement and regulation of digital health privacy

FTC and OCR

One overarching theme in digital health privacy is the overlapping jurisdiction of:

- The Federal Trade Commission (FTC), the U.S. privacy regulator with the broadest purview
- The Dept. of Health and Human Services (HHS), 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

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

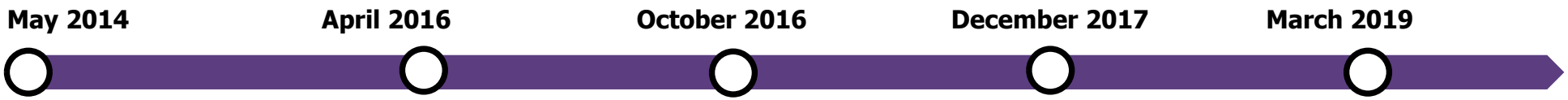
- An inaccurate or misleading statement or omission in a privacy policy, user interface or in other consumer-facing material can constitute a deceptive practice

In 2005, FTC used the "unfairness doctrine" in an enforcement action involving BJ's Wholesale Club

- The unfairness doctrine allows 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

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 guidance for businesses selling genetic testing kits

FTC's Health Breach Notification Rule

- Pursuant to the HITECH Act, FTC issued a Health Breach Notification Rule in 2009
  - Generally, mirrors the HIPAA Breach Notification Rule
- Applies to:
  - A vendor of personal health records (PHRs)
  - A PHR-related entity
  - A third-party service provider for a vendor of PHRs or a PHR-related entity
- Vendors and PHR-related entities must notify affected persons, FTC and, in some cases, the media if there's a breach of unsecured, individually identifiable health information
  - Third-party service providers must provide upstream notification

FTC's Health Breach Notification Rule Policy Statement

- On September 15, 2021, FTC issued a new policy statement affirming that health apps and connected devices that collect or use health information must comply with the Health Breach Notification Rule
  - Requires that they notify consumers and, in some cases, the media when that data is disclosed or acquired without the consumer's authorization
  - Ensures that entities not covered by HIPAA face accountability when consumers' sensitive health information is breached

- FTC noted that health apps have a responsibility to ensure they secure the data they collect, which includes preventing unauthorized access to such information

FTC's Health Breach Notification Rule Policy Statement (cont.)

- The Rule covers vendors of personal health records that contain individually identifiable health information created or received by health care providers
- The developer of a health app or connected device is a "health care provider" because it "furnish[es] health care services or supplies"
- The Rule is triggered when such entities experience a "breach of security"
  - A "breach" is not limited to cybersecurity intrusions or nefarious behavior
  - Incidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule

FTC's Health Breach Notification Rule Policy Statement (cont.)

- The Rule covers apps and connected devices that collect consumers' health information if they draw data from multiple sources, and are not covered by a similar rule issued by HHS
  - For example, a health app would be covered under FTC's rule if it collects health information from a consumer and has the technical capacity to draw information through an API that enables synching with a consumer's fitness tracker
- The Rule covers an app that draws information from multiple channels, even if the health information comes from only one source
  - For example, a blood sugar monitoring app would be covered under FTC's rule if it draws health information only from one source (e.g., a consumer's inputted blood sugar levels), but also takes non-health information from another source (e.g., dates from your phone's calendar)
- Penalties of up to $43,792 per violation per day for non-compliance

FTC's Settlement with Flo Health, Inc.

- Flo Health, Inc. is a developer of a period and fertility-tracking app used by more than 100 million consumers
- In January 2021, FTC alleged in a complaint that Flo Health shared sensitive health data from millions of users with marketing and analytics firms, including Facebook and Google
  - Alleged affected data included name, email address, date of birth, place of residence, dates of menstrual cycles, when pregnancies started and ended, menstrual and pregnancy-related symptoms, weight, and temperature
  - Alleged Flo Health did not contractually limit how third parties could use data received from the app
  - Alleged the Terms of Service permitted the third parties to use the data for their own purposes
- On June 22, 2021, FTC finalized a settlement with Flo Health

FTC's Settlement with Flo Health, Inc. (cont.)

- Settlement Requirements
  - Notify affected users about the disclosure of their health information
  - Instruct any third party that received users' health information to destroy that data
  - Obtain the affirmative consent of users of the company's fertility-tracking app before sharing their personal health information with others
  - Obtain an independent review of privacy practices
  - Prohibited from misrepresenting:
    - Purposes for which it (or entities to whom it discloses) collect, maintain, use, or disclose the data
    - How much consumers can control these data uses
    - Its compliance with any privacy, security, or compliance program
    - How it collects, maintains, uses, discloses, deletes, or protects users' personal information

Healthcare Mobile Apps

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 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"

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

CCPA and New State Privacy Laws

- New consumer privacy laws have been passed in California, Virginia, Colorado, Utah and Connecticut
- Each of these laws includes an exception for HIPAA covered entities, business associates and/or PHI
- But digital health companies regulated by the FTC may also be subject to these laws
- FTC may apply its Section 5 regulatory authority to these detailed privacy policies mandated by the new state laws
- For digital health businesses that do not qualify for its HIPAA exception, the California Consumer Privacy Act imposes new requirements
  - A.B. 713 amendment, effective January 1, 2021, added new notice and contracting requirements regarding de-identified data

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 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?

EHR Access FAQ

An individual directs a covered entity to send ePHI to a designated app

- Is the EHR developer liable for HIPAA noncompliance after the transmission is completed?

Answer: It Depends

- The EHR developer is a business associate of the covered entity but does not otherwise have a relationship with the app
  - Then the developer would not be liable under HIPAA for subsequent use or disclosure of the ePHI received by the app
- If the EHR developer has a business associate relationship with the app developer and provides the app on behalf of a covered entity
  - Then the developer could be liable if the app impermissibly uses or discloses the ePHI received

OCR Request for Information (RFIs): HIPAA Recognized Security Practices

- On April 6, 2022, OCR released a Request for Information (RFI)
- OCR requested comment on how regulated entities are voluntarily implementing security practices under HITECH
  - Previously, on January 5, 2021, HITECH was amended to require HHS to consider recognized security practices covered entities and their business associates used when determining potential penalties
  - Sample questions
    - *"What recognized security practices have regulated entities implemented? If not currently implemented, what recognized security practices do regulated entities plan to implement?"*
    - *"What steps do covered entities take to ensure that recognized security practices are actively and consistently in use continuously over a 12-month period?"*

Interoperability Rules Facilitate Patient Access

- On May 1, 2020, CMS and ONC released regulations to implement Cures Act requirements for interoperability and patient access. Both final rules note that patients should be able to use certified health IT to access their health records through health apps using secure, standards-based application programming interfaces (APIs)
  - This approach gives individuals the ability to electronically access and share their health information with mobile applications of their choice
  - The CMS interoperability and patient access final rule also requires CMS-regulated payers to make information available to patients using their choice of health apps. CMS-regulated entities must implement and maintain a standard-based Patient Access API to support data exchange and empower patients using apps.

Interoperability Implementation

July 1, 2021
CMS begins to enforce requirements for certain payers to support Patient Access and Provider Directory APIs.
ONC placed focus on HIPAA definition of "designated record set"

April 30, 2021
Hospitals with certain EHR capabilities must send admission, discharge and transfer notifications to their providers

September 2021
CMS announces that payer-to-payer data exchange provisions will not be enforced until future rulemaking is finalized

Information Blocking Rule

- What individuals and entities are subject to the information blocking regulations ("actors")?
  - Health IT developers of Certified Health IT
  - Health Information Networks (HINs) & Health Information Exchanges (HIEs)
  - Health Care Providers

- "Interfere with" or "interference" means to prevent, materially discourage, or otherwise inhibit
  - A provider could be engaging in information blocking if it refuses to respond to a request from a health app selected by the patient

COVID-19 and Privacy: OCR

- COVID-19 has raised a host of new privacy issues
- OCR has issued a series of COVID-related guidance documents
  - Notable for digital health: March 17, 2020 Notice of Enforcement Discretion for Telehealth Remote Communications
    - Waives potential HIPAA penalties for HIPAA violations against health care providers that serve patients through "everyday communications technologies," such as Zoom, Skype and Google Hangouts video
    - Can use any non-public facing remote communication product that is available to communicate with patients
    - OCR also issues related FAQ guidance on telehealth
- OCR enforcement discretion guidance will terminate when federal declaration of COVID as a public health emergency terminates

OCR Right of Access Initiative

- Announced in February 2019
- Individuals have a right to timely access their health records, and at a reasonable, cost-based fee
- Investigations launched across the country
- 27 settlements to date

HIPAA Notice of Proposed Rulemaking (NPRM)

- On December 11, 2020, OCR issued a Notice of Proposed Rulemaking that would amend the HIPAA Privacy Rule
  - OCR is currently considering comments submitted
- NPRM largely deals with coordination of care issues
  - Part of HHS effort to promote value-based care
- Because it is most relevant to digital health, we'll discuss the NPRM's proposals regarding access to PHI

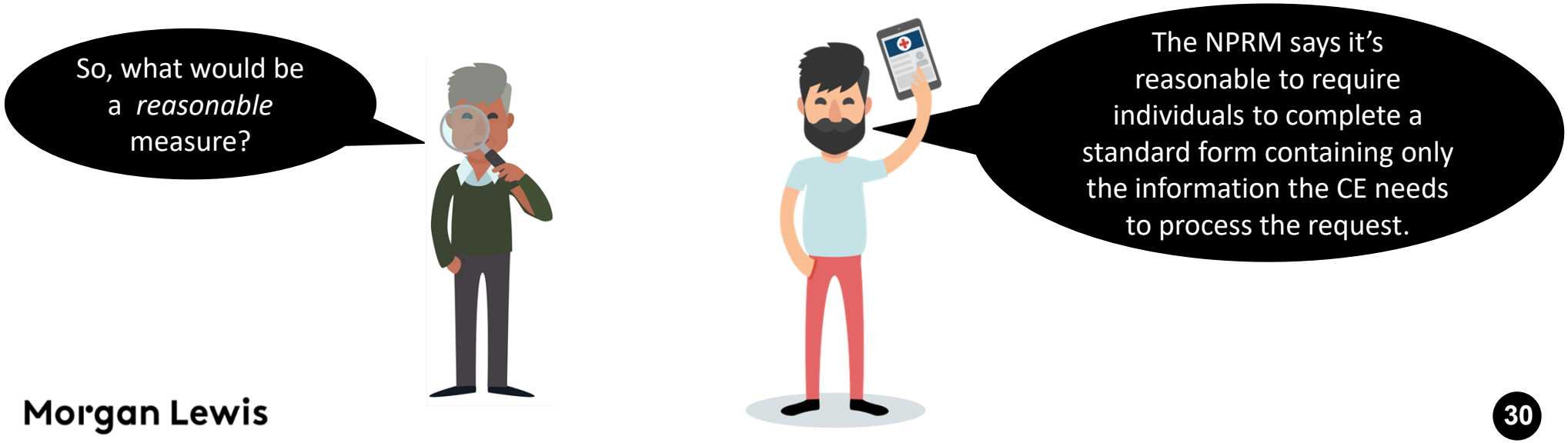
Time to Act on Requests for Access

- "As soon as practicable" but no later than 15 calendar days after receipt of request

- One possible extension of 15 calendar days, provided that the covered entity has implemented a policy to prioritize urgent or otherwise high priority requests (especially those relating to the health and safety of individual or another person)

Access Request Measures

- A covered entity may require access requests in writing, but only if the covered entity:
  - Informs the individual of the requirement
  - Does not impose unreasonable measures impeding the individual from obtaining access when a less burdensome measure is practicable for the CE



Identity Verification Measures

- Current identity verification requirements remain
- Prohibition on unreasonable identity verification requirements for individuals attempting to exercise their rights under the HIPAA Rules, including the right of access
- Unreasonable measures cause an individual to expend unnecessary effort or resources when a less burdensome verification measure is practicable for the covered entity

Right to Inspect

- Right to view, take notes and photographs, and use other personal resources to capture their PHI in a designated record set at a mutually convenient time and place, including in conjunction with a health care appointment

- A covered entity may establish limits:
  - Not required to allow connection of personal devices to CE's information systems
  - May impose measures to ensure individual only records PHI to which individual has right of access
  - May establish reasonable policies and safeguards to minimize disruption to operations

Form and Format

- Deem PHI "readily producible" in an electronic form and format where another applicable federal or state law requires that form and format

- If a covered entity or its EHR developer (business associate) has implemented a secure, standards-based API that is capable of providing access to ePHI in the form and format used by an individual's personal health application, that ePHI is considered to be *readily producible* in that form and format

Definition of Personal Health App

Personal health application means an electronic application used by an individual→

- to access health information about that individual,
- which can be drawn from multiple sources,
- provided that such information is managed, shared, and controlled by or primarily for the individual, and *not* by or primarily for a covered entity or another party such as the application developer.

Definition of Electronic Health Record

- **EHR:** An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and their staff

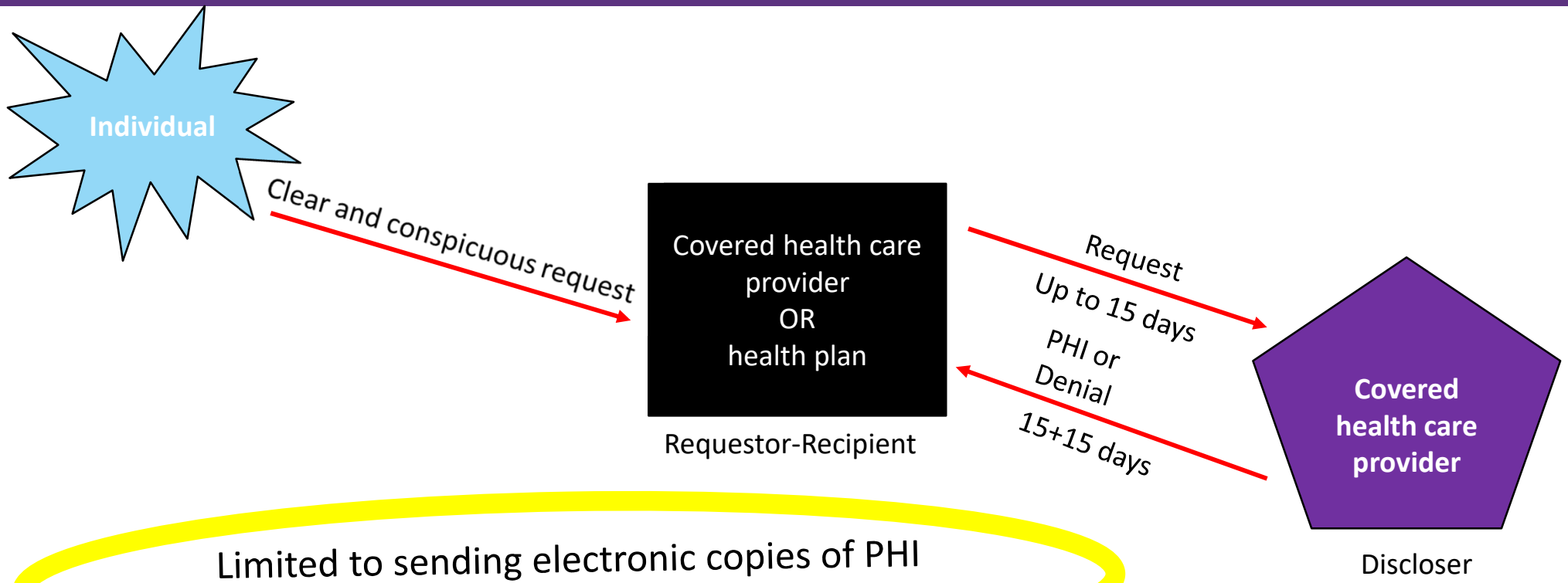
  - **Clinicians:** Health care providers that have a *direct treatment relationship* with individuals

  - **Health-related information on an individual:** *Individually identifiable health information*

Right to Direct ePHI to a Third Party

- Right to direct a ***covered health care provider*** to transmit an ***electronic copy*** of PHI ***in an EHR*** to a third party
- "Clear, conspicuous, and specific" request
  - Orally or in writing (which may be electronically executed)
  - Individual may use an internet-based method, such as a *personal health application*, *to submit the access request*, so long as it is "clear, conspicuous, and specific"

Right of Access to Direct Disclosures



Limited to sending electronic copies of PHI in EHR to Requestor-Recipient

Wellness Programs

- Healthcare mobile apps are being offered as part of some workplace wellness programs

Are such apps regulated by OCR or FTC?

  - If the wellness program app is offered through the employer's group health plan?
  - If the wellness program app is offered directly by the employer?

- See "HIPAA Privacy and Security and Workplace Wellness Program" at HHS.gov

Personal Health Records

What is a Personal Health Record (PHR)?

No universally accepted definition

- However, this definition from HITECH and FTC Breach Notification Rule is as good as any: "The term 'personal health record' means an electronic record of PHR identifiable health information (as defined in section 17937(f)(2) of this title) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."

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

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!

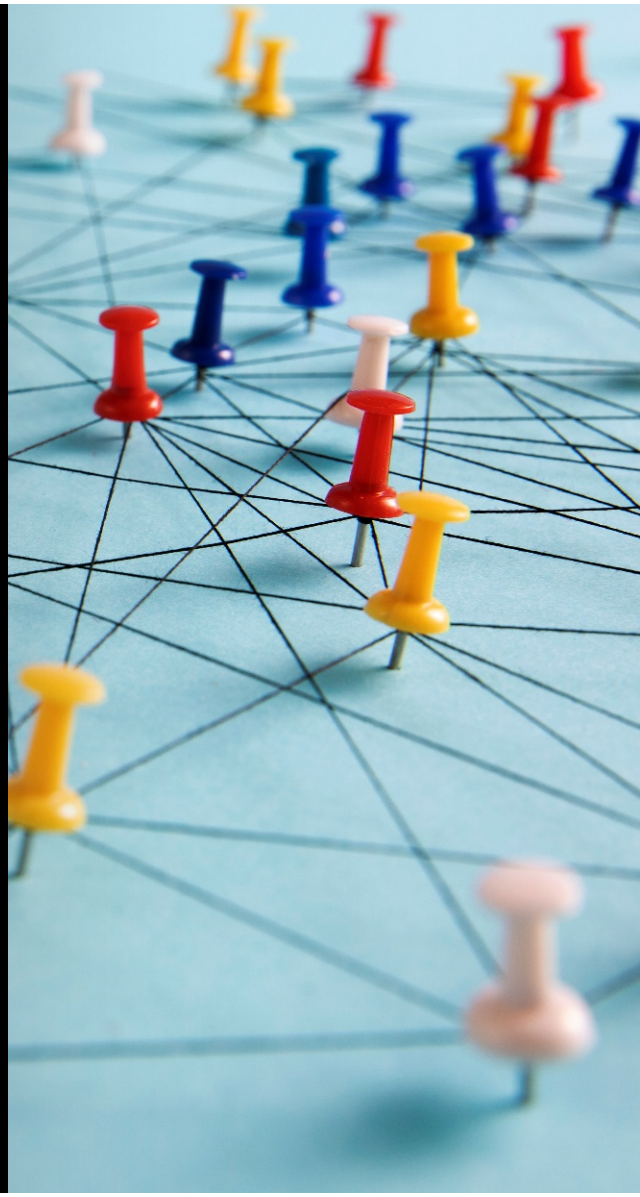
Ukraine Conflict Resources

Our lawyers have long been trusted advisers to clients navigating the complex and quickly changing global framework of international sanctions. Because companies must closely monitor evolving government guidance to understand what changes need to be made to their global operations to maintain business continuity, we offer a centralized portal to share our insights and analyses.

Morgan Lewis

To help keep you on top of developments as they unfold, visit the website at www.morganlewis.com/topics/ukraine-conflict

To receive a daily digest of all updates, please visit the resource page to subscribe using the "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.

SYDNEY REED SWANSON

Sydney Reed Swanson
Houston
+1.713.890.5105
sydney.swanson@morganlewis.com

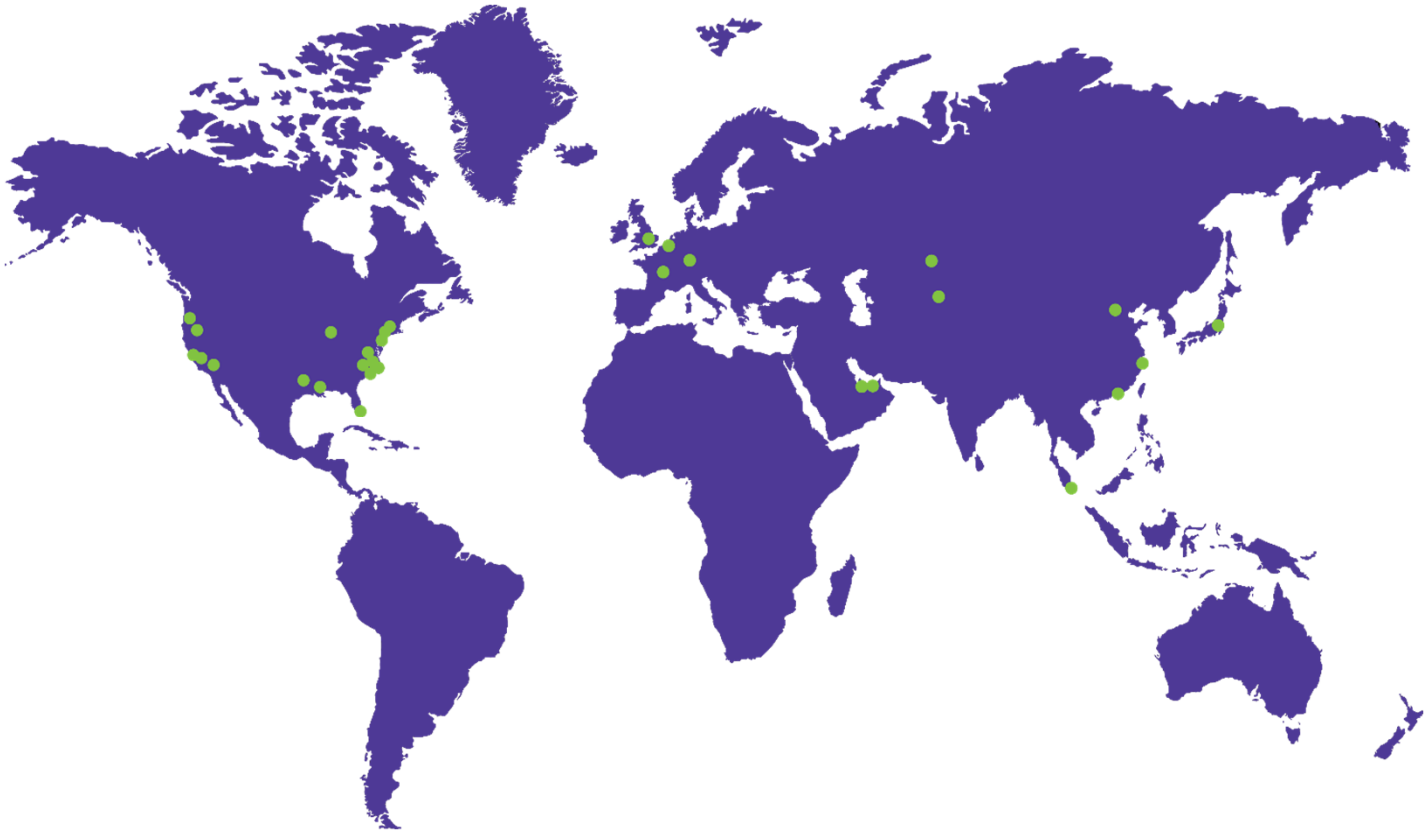
Sydney Reed Swanson focuses her practice on reimbursement issues and disputes; transactional, regulatory, and compliance matters; government investigations and litigation involving federal and state False Claims Act (including *qui tam* claims) and Anti-Kickback Statute physician self-referral (Stark Law) matters; and appeals before the Provider Reimbursement Review Board (PRRB) and the Office of Medicare Hearings and Appeals (OMHA). Sydney advises clients on many aspects of the coronavirus (COVID-19) pandemic, including federal, state, and local regulation of healthcare organizations pertaining to supply chain issues, price gouging, changes in provider scope of practice, and waivers of licensure and enrollment requirements.

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
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU