# 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
  - Offered as a basis for comment and response by the panelists
- Presenters:
  - Reece Hirsch, co-head of Privacy & Cybersecurity Practice, Morgan Lewis
  - Linda Sanches, Senior Advisor, Health IT and Privacy Policy, Office for Civil Rights, U.S. Department of Health and Human Services

# 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 telemedicine
  - 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

- This presentation will review the latest developments in HIPAA and OCR enforcement, with a focus on digital health

# 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
- 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, 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 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 guidance for businesses selling genetic testing kits

# 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 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
- 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 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?

# 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

# 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

- September 2021: CMS announces that payer-to-payer data exchange provisions will not be enforced until future rulemaking is finalized
- April 30, 2021: Hospitals with certain EHR capabilities must send admission, discharge and transfer notifications toother providers
- July 1, 2021: CMS begins to enforce requirements for certain payers to support Patient Access and Provider Directory APIs
  - Has placed focus on HIPAA definition of "designated record set"
- Information blocking rule

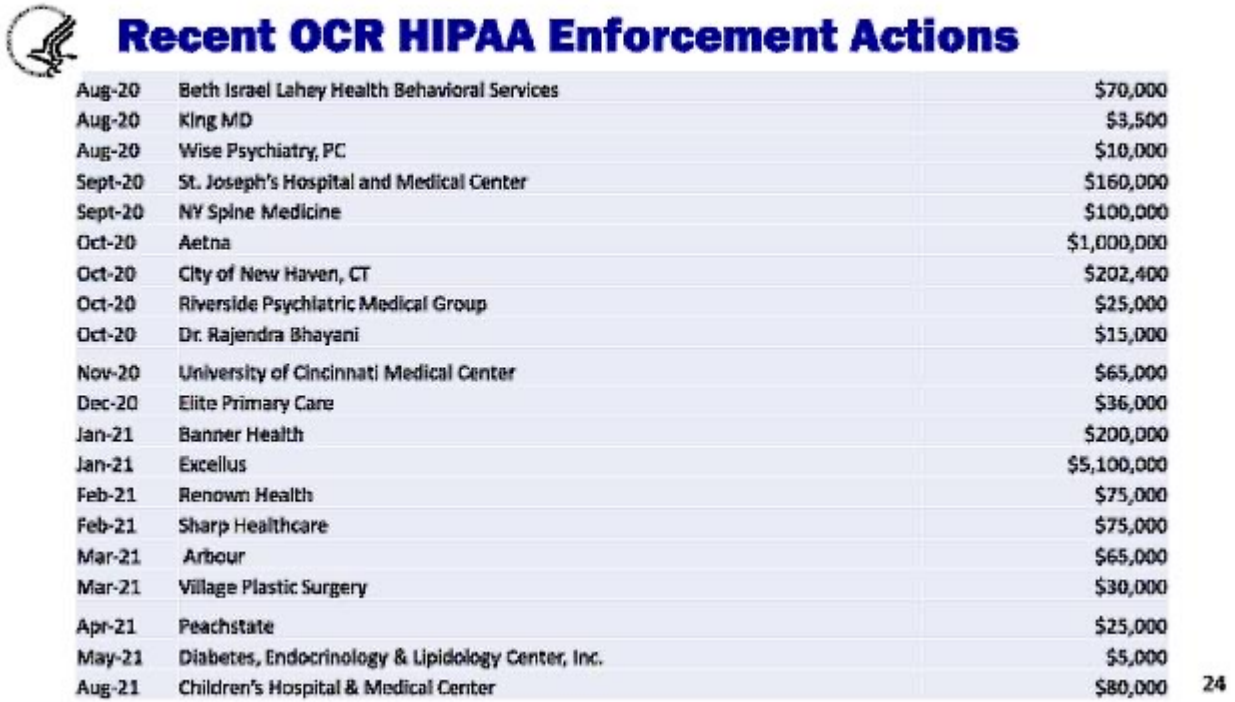
# COVID-19 and Privacy: OCR

- 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 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

# The Regulatory Landscape

- What is the outlook of OCR with respect to the digital health privacy space?
- Guidance documents in the pipeline?
- Areas of likely enforcement or concern?
- For digital health businesses that do not qualify for its HIPAA exception, the California Consumer Privacy Act imposes new requirements
  - A.B. 713 amendment, signed into law on Sept. 29, 2020, added new notice and contracting requirements regarding de-identified data

# Recent OCR HIPAA Enforcement Actions



## Recent OCR HIPAA Enforcement Actions

| | | |
|---|---|---|
| Aug-20 | Beth Israel Lahey Health Behavioral Services | $70,000 |
| Aug-20 | King MD | $3,500 |
| Aug-20 | Wise Psychiatry, PC | $10,000 |
| Sept-20 | St. Joseph's Hospital and Medical Center | $160,000 |
| Sept-20 | NY Spine Medicine | $100,000 |
| Oct-20 | Aetna | $1,000,000 |
| Oct-20 | City of New Haven, CT | $202,400 |
| Oct-20 | Riverside Psychiatric Medical Group | $25,000 |
| Oct-20 | Dr. Rajendra Bhayani | $15,000 |
| Nov-20 | University of Cincinnati Medical Center | $65,000 |
| Dec-20 | Elite Primary Care | $36,000 |
| Jan-21 | Banner Health | $200,000 |
| Jan-21 | Excellus | $5,100,000 |
| Feb-21 | Renown Health | $75,000 |
| Feb-21 | Sharp Healthcare | $75,000 |
| Mar-21 | Arbour | $65,000 |
| Mar-21 | Village Plastic Surgery | $30,000 |
| Apr-21 | Peachstate | $25,000 |
| May-21 | Diabetes, Endocrinology & Lipidology Center, Inc. | $5,000 |
| Aug-21 | Children's Hospital & Medical Center | $80,000 |

24

# 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
- Twenty settlements to date

# HIPAA Notice of Proposed Rulemaking (NPRM): Selected Topics

- Right of Access
- Care Coordination and Exception to Minimum Necessary Standard
- Disclosures to Facilitate Care with Social and Community-Based Services
- Telecommunications Relay Services

# Definition of Personal Health App

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

- to access health information a that individual,
- which can be drawn from mult 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.

# 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 (esp. those relating to the health and safety of individual or another person)

- Shorter timelines in other law are "practicable"

# 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 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

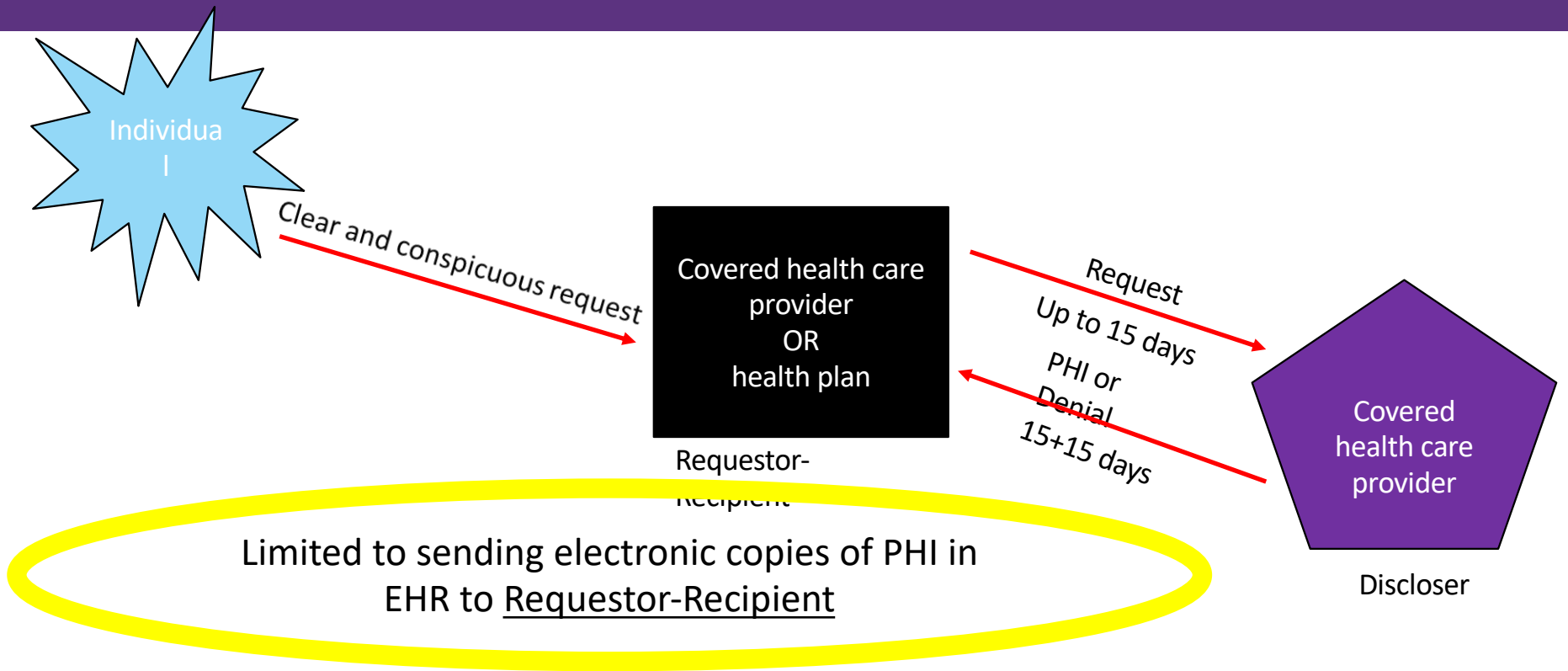
  - **Clinicians:** Health care providers that have a *direct treatment relationship* with individuals

  - **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



# Exception to Minimum Necessary Standard

- Exception to the minimum necessary standard for disclosures to, or requests by, a health plan or covered health care provider for care coordination and case management for individuals

- Exception would not apply to population-based care coordination and case management

- Covered entities would still be able to honor individuals' requests for privacy restrictions

# Care Coordination Disclosures to Third Parties

- Express permission for covered entities to disclose PHI to third parties for care coordination and case management with respect to an individual
  - Social services agencies
  - Community-based organizations
  - Home and community-based services providers (HCBS)
  - Similar third parties that provide or coordinate health-related services
- Individuals can still request restrictions on disclosures of PHI for treatment, payment, and health care operations

# Telecommunications Relay Service (TRS)

- Expressly permit disclosures to TRS communications assistants for persons who are deaf, hard of hearing, or deaf-blind, or who have a speech disability

- Exclude TRS providers from the definition of *business associate*

- Ensure that workforce members of a covered entity or business associate can use TRS to share PHI with other workforce members or outside parties as needed to perform their duties

# Wellness Programs

- Healthcare mobile apps are being offered as part of some workplace wellness programs
- Are such apps regulated by OCR or the 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 the HITECH Act and the 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

# FTC's Health Breach Notification Rule

- Pursuant to HITECH, the FTC issued a Health Breach Notification Rule in 2009
  - Generally 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
- Vendors and PHR-related entities must notify affected persons, the 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
- September 15, 2021: FTC issues statement affirming that rule applies to health apps and connected devices that collect health information

# 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!