Morgan Lewis

TECHNOLOGY MARATHON

The Growing Complexities of Regulating Digital Healthcare Products

W. Reece Hirsch and Sydney Reed Swanson

Monday, May 8th | 1:00 pm ET

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

- **Implementation of the CMS and ONC interoperability rules is facilitating patient access to PHI**
- **Continued proliferation of digital health mobile apps, wearables and Internet of Medical Things (IoMT) devices**
- **Continued development of artificial intelligence (AI) and applications of AI**
- **Change in law related to privacy and reproductive health information**

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

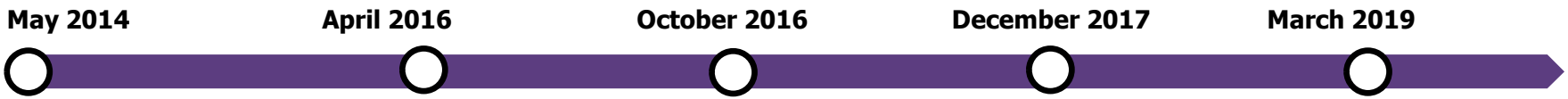
- An inaccurate or misleading statement or omission in a privacy policy, user interface or in other consumer-facing material can constitute a deceptive practice

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, triggerh 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 GoodRx

- FTC's first action alleging a violation of the Health Breach Notification Rule
- GoodRx Holdings, Inc. is a digital health platform that allows consumers to compare prescription drug prices and get prescription drug coupons
- On February 1, 2023, FTC alleged in a complaint that GoodRx:
  - Collected health information through online tracking technologies and then disclosed that information for marketing and other purposes, despite its assurances that it would not
  - Failed to notify users that it had disclosed their health information to third parties without their consent
- On February 17, 2023, FTC entered a stipulated order to settle the matter
  - $1.5 million penalty
  - A novel remedy – prohibition on GoodRx from sharing user health data with applicable third parties for advertising purposes

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 key 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?"
  - A business associate must be "acting on behalf of" a HIPAA covered entity, not on behalf of a consumer/patient
  - 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

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?

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

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

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"

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 exchange or use of electronic health information (EHI)
  - A provider could be engaging in information blocking if it refuses to respond to a request from a health app selected by the patient
  - An app developer could be engaging in information blocking if it makes it more difficult for a user to share EHI with another app

CCPA and New State Privacy Laws

- New consumer privacy laws have been passed in California, Virginia, Colorado, Utah, Connecticut
- Each of these laws includes an exception for HIPAA covered entities, business associates and/or PHI
- 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

Washington's My Health, My Data Act

- On April 27, 2023, Washington Gov. Jay Inslee signed into law the My Health, My Data Act
  - A game-changing state law regulating digital health companies
  - Effective March 31, 2024 (June 30, 2024 for small businesses)
- Intended to regulate consumer health data maintained by entities not regulated by HIPAA
- Regulated entities subject to the Act include any entity that
  - Has a commercial nexus to Washington and
  - "Determines the purpose and means of collecting, processing, sharing or selling of consumer health data"

Washington's My Health, My Data Act (cont.)

- **"Consumer health data"** is broadly defined to include any "personal information that is linked or reasonably linkable to a consumer and that identifies a consumer's past, present, or future physical or mental health," including
  - Precise location data that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies
  - Health-related information that is derived or extrapolated from nonhealth information
- Consumers protected by the Act include Washington residents and individuals "whose consumer health data is collected in Washington"

My Health, My Data Act Requirements

- **Consent:** Regulated entities must obtain separate consents before collecting or sharing a consumer's health data (unless the collection or sharing is necessary to provide a product or service requested by the consumer)
  - "Consent" means "a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary and unambiguous agreement"
- **Sales:** Sale of consumer health data requires a "valid authorization" from the consumer
  - "Sale" is broadly defined as "the exchange of consumer health data for monetary or other valuable consideration"

My Health, My Data Act: Policies, Data Rights

- Regulated entities must maintain and publish consumer health data policies that disclose:
  - Categories of consumer health data collected and the purpose for which the data was collected and how it will be used and shared
  - Categories of third parties and affiliates with whom the entity shares consumer health data
  - How a consumer can exercise relevant rights under the Act
- The Act creates rights for consumers, including
  - Right to confirm whether a regulated entity is collecting, sharing or selling an individual's health data and to access that data
  - Right to withdraw consent for the collection and sharing of consumer health data
  - Right to delete consumer health data

My Health, My Data Act

- **Security:** Regulated entities must implement data security practices sufficient to satisfy a "reasonable standard of care" within its industry
- **Geofencing Restrictions:** The Act prohibits geofencing around entities that provide in-person health care services when the geofence is used to
  - Identify or track consumers seeking health care services
  - Collect consumer health data
  - Send messages or ads to consumers regarding consumer health data or health care services
- **Enforcement:** The Act is enforceable by the WA Attorney General and there is a private right of action under the WA Consumer Protection Act

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?

AI and Healthcare Privacy

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

Is AI Processing a "Use" of PHI?

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

Is AI Processing a Permitted Purpose Under HIPAA?

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

Is Development of AI a Research Activity?

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

AI Processing By HIPAA Business Associates

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

AI and FTC Privacy Regulation

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

HTI-1 Rule and AI

- April 18, 2023: the HHS Office of the National Coordinator of Healthcare Technology issued a proposed rule that begins to define how the federal government will regulate use of AI/ML in healthcare
  - The Health Data, Technology and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing proposed rule (HTI-1)
- HTI-1 outlines a number of new and updated criteria for a health information technology developer to have health IT certified under the Office of the National Coordinator Health IT Certification Program, which is voluntary
- HTI-1 focuses on assessing whether predictive decision support interventions (DSIs) adhere to fair, appropriate, valid, effective and safe (FAVES) principles

HTI-1 and AI (cont).

- Three categories of FAVES:

1. Providing technical and performance information to users of DSIs
2. Requiring developers of DSIs to follow a range of risk management practices
3. Requiring developers of DSIs to participate in real-world testing

- Under the proposed rule, health IT developers would need to attest "yes" or "no" as to whether their health IT module enables or interfaces with one or more predictive DSIs

Healthcare Privacy and Reproductive Health

In July 2022, FTC published a blog warning companies it will take enforcement action against conduct that exploits users' location and other health data.

In August 2022, FTC filed an enforcement action against Kochava for selling geolocation data in a manner that constitutes unfair business practices.

In June 2022, OCR issued guidance discussing the role that HIPAA plays in safeguarding the PHI of women and how individuals can safeguard data on personal devices.

In April 2023, OCR published a proposed rule to modify HIPAA with the goal of strengthening reproductive healthcare privacy.

FTC Post-*Dobbs*

- In July 2022, the Biden administration issued an executive order on abortion access, in which it asked the FTC to take steps to protect abortion data privacy
- Days later, FTC issued a blog post warning companies and data brokers that it would crack down on any illegal conduct that exploits users' location, health, or other sensitive data
  - Highlighted that information related to personal reproductive matters may be particularly at risk of misuse
  - Including information collected by products that track women's periods, monitor their fertility, oversee their contraceptive use, or even target women considering abortion
  - Stated that the exposure of health information, especially data related to sexual activity or reproductive health, may subject people to discrimination, stigma, mental anguish, or other serious harms

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, requiring changes in business practices and compliance efforts

FTC's Case Against Kochava

- Kochava Inc. is an Idaho-based data broker
- In August 2022, FTC alleged in a complaint that Kochava sold geolocation data from millions of mobile devices in a manner that constitutes unfair business practices
  - Alleged that the data can be used to trace the movements of individuals to and from sensitive locations
  - Alleged the data could be used to identify people who have visited a reproductive health clinic and expose their private medical decisions
  - Alleged the data may be used to track a mobile device from a reproductive health clinic to a single-family residence to other places routinely visited
  - Alleged the data may be used to identify medical professionals who perform reproductive health services
- May 4, 2023: Idaho federal judge granted Kochava's motion to dismiss the FTC's suit, but gave FTC leave to amend

OCR Post-*Dobbs*

- On June 29, 2022, OCR issued guidance discussing the role that HIPAA plays in safeguarding the protected health information of women
  - "Permissions for disclosing PHI without an individual's authorization for purposes not related to health care … are narrowly tailored to protect the individual's privacy and support their access to health services."
  - In discussing HIPAA exceptions for disclosures (1) required by law, (2) for law enforcement purposes and (3) to avert a serious threat to heath or safety, OCR emphasizes that HIPAA permits but does not require these disclosures.
- Example: A woman goes to a hospital experiencing a miscarriage. Even if the hospital worker suspects that the woman took medication to end her pregnancy in violation of state law, if the state law does not expressly require such reporting, the hospital worker may not report the patient to law enforcement.

OCR Post-*Dobbs*

- Nothing in the OCR Dobbs guidance alters the HIPAA disclosure rules, but it does suggest that OCR intends to interpret HIPAA in a manner that favors safeguarding access to abortion and reproductive health services.
- If a HIPAA covered entity opposes a requested disclosure of reproductive health information from a law enforcement agency or other third party, OCR seems unlikely to pursue that conduct as a HIPAA violation.
  - This doesn't mean that HIPAA covered entities might not face potential liability under state law causes of action, such as "aiding and abetting" abortion services in states in which those services are illegal.

OCR Post-*Dobbs*

- On June 29, OCR also issued the guidance, "Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet."
  - Unlike the HIPAA privacy guidance, OCR focuses on the activity of individual patients rather than covered entities.
  - Recognizes that health information collected through an individual's personal devices, such as cell phones or tablets, is generally not subject to HIPAA protections.
  - FTC privacy principles generally apply to "direct-to-consumer" digital health products.
  - Unless they are provided through a HIPAA covered entity.

- Personal devices often collect geolocation data, Internet search history, and private messages –all of which may be considered evidence of violations of state reproductive health laws.

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
- Be prepared for Washington's My Health, My Data Act in 2024!

Remember that many digital health companies straddle multiple privacy and security regulatory regimes

KNOW WHEN YOU'RE CROSSING ONE OF THOSE LINES!

Your CLE Credit Information

For ALL attorneys seeking CLE credit for attending this webinar, please write down the alphanumeric code on the right >>

Kindly insert this code in the **pop-up survey** that will appear in a new browser tab after you exit out of this webinar.

THE CLE CODE IS:

DW432QA

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. In a Chambers USA ranking, Reece was recognized by his peers as "a consummate expert in privacy matters."

SYDNEY REED SWANSON

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

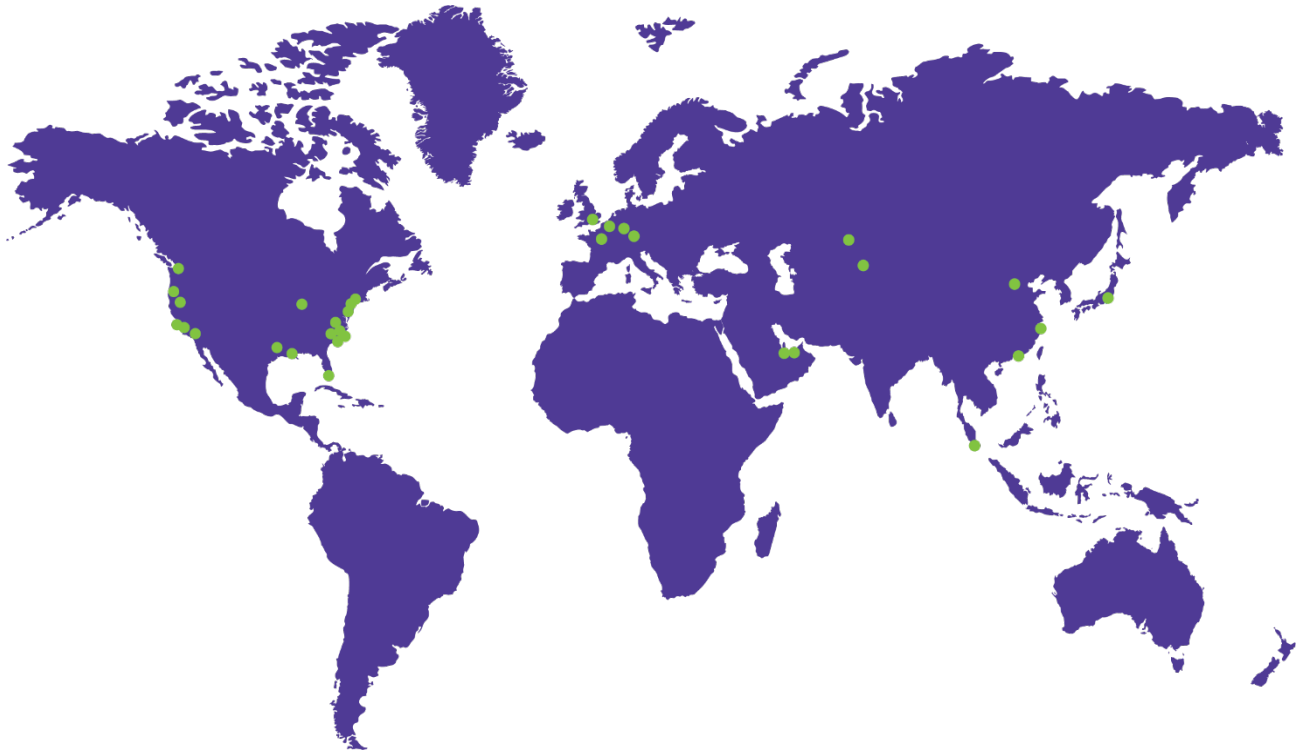
Sydney Reed Swanson focuses her practice on the application of healthcare regulatory and healthcare privacy law to transactional, regulatory, and compliance matters. Sydney counsels clients on healthcare privacy and security matters, such as compliance with the Health Insurance Portability and Accountability Act (HIPAA) and state medical privacy laws. Sydney represents healthcare industry clients in relation to False Claims Act litigation, state and federal government investigations, overpayment disputes and demands, and regulatory enforcement proceedings, including civil monetary penalties related to HIPAA.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

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



Morgan Lewis

THANK YOU