Morgan Lewis

# NEW DEVELOPMENTS IN HIPAA REGULATION AND ENFORCEMENT

## LOOKING BACK AT 2017, WHAT TO EXPECT IN 2018

Reece Hirsch

January 17, 2018

# Looking Back, Looking Forward

- 2017 was another noteworthy year for HIPAA enforcement and regulation
  - Major settlements
  - The conclusion of the Phase 2 audits
  - New guidance on a number of topics, including
    - Responding to cyberattacks
    - Disclosures of PHI in the context of the opioid crisis
    - Disclosures of PHI during disasters, such as hurricanes and mass shootings
  - Year was perhaps most notable for what did NOT happen (at least during the last six months)

# Is HIPAA Enforcement on Pause?

- Until late December, the Office for Civil Rights (OCR) had gone nearly six months without a health data breach settlement
- 2016: 13 reported resolution agreements totaling nearly $25 million in penalties
- January–May 2017: 9 resolution agreements totaling nearly $18 million in penalties
  –OCR was on track for a record year for HIPAA enforcement
- June 2017 –December 27, 2017: 0 resolution agreements
- Is this the new OCR?

# Is HIPAA Enforcement on Pause? (cont.)

- In November 2017, Deven McGraw, former deputy director for health information privacy at OCR, stated that this pause does not reflect a pullback in enforcement
  - Lag is more the result of the change in administration and new OCR Director Roger Severino settling into his position
  - More data breach settlements in the near future
  - Severino has "the pedal to metal on enforcement"

- The Fiscal Year 2018 budget request for OCR is $33 million, $6 million below the 2017 level
  - FTEs would be reduced by 17 from 179 to 162
  - OCR "will reduce overhead and non-personnel costs"
  - Civil monetary settlement funds will be used to support OCR enforcement activities

- Outlook is unclear for OCR's HIPAA enforcement in 2018

# Recent OCR Enforcement Actions: Presence Health

- January 9, 2017: $475,000 settlement with Presence Health Network, one of largest Illinois health systems
  - First time OCR enforcement action has been based on failing to comply with breach notification requirements
  - Paper-based operating room records of 836 patients went missing
  - Presence failed to comply with 60-calendar-day breach notification timing standard
  - Notified OCR 101 days after discovery, individuals (104 days), media (106 days)
  - Don't delay notification because investigation of the breach is still uncovering new information
    - OCR breach notification process permits an addendum notification
    - During investigation, OCR noted other occasions where Presence was late in notifying individuals of breaches of less than 500 (compliance history is important!)
  - Each day notification is late is a separate violation of the Breach Notification Rule!

# MAPFRE Life Insurance Company of Puerto Rico Settlement

- January 18, 2017:  OCR announces $2.2 million settlement with MAPFRE Life Insurance Company of Puerto Rico
- In September 2011, a data storage device was stolen from IT department
  - Device contained information of 2,209 individuals
- Insurer represented to OCR that it would implement a security risk analysis and risk management plan and employ encryption of portable devices
  - Failed to do so until September 2014
  - OCR Director Jocelyn Samuels: "Covered entities must not only make assessments to protect ePHI, they must act on those assessments as well."

# Memorial Healthcare System Settlement

- February 16, 2017: OCR announces $5.5 million settlement with Memorial Healthcare System, which operates 6 hospitals and other facilities in South Florida
  - MHS reported to OCR that PHI of 115,143 individuals had been impermissibly accessed by its employees and disclosed to affiliated physician office staff
  - Login credentials of a former employee of a physician office had been used to access ePHI on a daily basis without detection from April 2011 to April 2012
  - MHS had workforce access policies and procedures in place, but failed to review information system activity
    - Despite having identified this risk on several risk analyses from 2007–2012
  - Takeaway: Organizations must implement audit controls and review audit logs regularly
    - Failure to do so allows hackers and bad actors to cover their tracks, making it difficult to recover from and prevent breaches

# Metro Community Provider Network Settlement

- April 12, 2017: OCR announces a $400,000 settlement with Metro Community Provider Network (MCPN), a federally-qualified health center in the Denver area
  - In January 2012, MCPN filed a breach report indicating that a hacker accessed employees' email accounts and obtained 3,200 individuals' ePHI through a phishing scheme
  - MCPN took necessary corrective action in response to the breach
  - However, investigation revealed that MCPN failed to conduct a risk analysis until February 2012
  - Even after risk analyses were conducted, OCR concluded that they failed to meet HIPAA Security Rule requirements
  - Security risk analysis deficiencies: the biggest recurring theme in recent OCR HIPAA enforcement

# Center for Children's Digestive Health Settlement

- April 17, 2017: Center for Children's Digestive Health (CCDH), an Illinois pediatric digestive health practice, paid OCR $31,000 in a HIPAA settlement
  - CCDH disclosed PHI of at least 10,728 patients to document storage company FileFax, Inc. without obtaining a written business associate agreement
  - Related to a suit by IL AG Lisa Madigan charging that FileFax exposed thousands of patient records
    - Hundreds of files containing complete medical records were allegedly discovered in a dumpster outside FileFax's office
- CCDH is required to establish a process for assessing current and future relationships to determine whether each is a BA
  - Also requires procedures for limiting disclosures of PHI to BAs to the minimum necessary

# CardioNet Settlement

- April 24, 2017: $2.5 million settlement agreement with CardioNet, a wireless cardiac monitoring service provider, arose from a breach
  - The first OCR settlement with a wireless health provider
  - Workforce member's laptop was stolen from a parked vehicle outside the employee's house, containing ePHI of 1,391 individuals
  - OCR investigation concluded that CardioNet had an insufficient risk analysis and risk management process in place at the time of the event
  - Resolution agreement alleged that CardioNet had not fully implemented its HIPAA Security Rule policies and procedures, which were in draft form
    - Including the policies relating to mobile devices
    - Is your incident response plan fully approved, adopted, and implemented?

# Large SW Health System Settlement

- May 10, 2017:  OCR announces $2.4 million settlement with Health System
  - Health System disclosed the name of a patient who used a false identification card to the public and media
  - Disclosure was permissible to law enforcement, but not to the public
  - Hospital system allegedly sent a press release with patient's name to 15 reporters and news outlets, disclosed the name during meetings with advocacy groups and state lawmakers, and posted a news release with the name on its website
  - OCR also said that the hospital system didn't properly document how it sanctioned its employees for the improper disclosures
- Patient was arrested in September 2015 for providing false identification at a Health System clinic

# St. Luke's-Roosevelt Hospital Center Settlement

- May 23, 2017: OCR announces $387,000 settlement with St. Luke's-Roosevelt Hospital Center, Inc.
- Incident arose from a September 2014 patient complaint at the Institute for Advanced Medicine, which treats chronic diseases like HIV
- Investigation revealed that PHI of 2 patients was faxed to people who did not have a right to see it
  - One patient's information was sent to the patient's employer rather than to a designated personal P.O. box
  - One patient's information was sent to a place where the patient volunteered
- OCR stated that the sensitivity of the information about HIV, AIDS, and mental health made the impermissible disclosures egregious
- OCR cites lack of "reasonable safeguards"

# 21st Century Oncology Settlement

- December 28, 2017:  OCR enters into a $2.3 million settlement with 21st Century Oncology, Inc. (21CO), a chain of 179 cancer treatment centers based in Fort Myers, Florida
- On two occasions in 2015, the FBI notified 21CO that patient information was illegally obtained by an unauthorized third party and produced patient files purchased by an FBI informant
- 21CO's investigation determined that an attacker had accessed its network through the remote desktop protocol from an exchange server within 21CO's network
- 2.21 million patients were affected
- In May 2017, 21CO filed for Chapter 11 bankruptcy
  - OCR's corrective action plan was intended to ensure that organization emerges from bankruptcy with a strong HIPAA compliance program in place

# 21st Century Oncology Settlement (cont.)

- OCR investigation found that 21CO failed to:
  - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to ePHI
  - Implement procedures to regularly review records of information system activity, such as
    - Audit logs
    - Access reports
    - Security incident tracking reports
  - Enter into business associate agreements with vendors receiving PHI

# OCR Corrective Action Plans

- Each of the settlement agreements includes a corrective action plan (CAP) with OCR, which typically includes
  - A 2-year term
  - Completion of a security risk analysis and risk management plan
  - Revisions to certain affected policies and procedures and review by OCR
  - Adoption and distribution of final policies and procedures
  - An internal monitoring plan approved by OCR
  - Selection and engagement of a third-party assessor to review compliance with the CAP
  - Submission of written assessor reports to OCR
  - Annual reports to OCR during CAP period regarding compliance with the CAP

# OCR Urges Cyber Threat Monitoring

- February 2017: OCR releases guidance on reporting and monitoring cyber threats
  - In response to the September 2016 Government Accountability Office (GAO) report that data breaches impacting health care records of 500 or more individuals increased from 10 in 2010 to 56 in 2015, and recommending updated OCR guidance for protecting ePHI
  - Guidance recommends that CEs and BAs report suspicious activity, including cybersecurity incidents, cyber threat indicators, phishing incidents, and similar events to the United States Computer Emergency Readiness Team (US-CERT)
    - A branch of the National Cybersecurity and Communications Integration Center within Dept. of Homeland Security

# OCR Urges Cyber Threat Monitoring (cont.)

- However, disclosures of PHI to US-CERT must still fit within a HIPAA disclosure exception
  - Disclosures for national security and intelligence activities? 45 C.F.R. § 164.512(k)(2)
  - Nature of threat may often be shared without sharing PHI

- OCR recommends that CEs and BAs monitor US-CERT's website and sign up for email alerts for reports on current threats and for prompt access to patches and mitigations, when available
  - Good advice
  - This is the kind of up-to-date threat information that organizations should be incorporating into their periodic HIPAA security risk assessments

# OCR's Cyberattack Response Checklist

- In June 2017, OCR released a Quick-Response Checklist for cyberattacks
- The guidance is high-level and not particularly surprising
- OCR states that entities experiencing a cyberattack "should" report the crime to law enforcement agencies, which may include
  - State or local law enforcement
  - FBI
  - Secret Service
- However, the decision to report to law enforcement is not always so clear-cut
  - Will law enforcement draw additional public attention to the incident?
  - Is a particular law enforcement agency likely to vigorously pursue your type of cyberattack?

# OCR's Cyberattack Response Checklist (cont.)

- Cyberattack checklist also states that entities should report all "cyber threat indicators" to federal and information-sharing and analysis organizations (ISAOs), including
  - Dept. of Homeland Security
  - HHS Assistant Secretary for Preparedness and Response
- Reports should not include PHI
- OCR considers all mitigation efforts taken by an entity in any breach investigation, including voluntary sharing of breach-related information with law enforcement agencies and ISAOs
- Not all HIPAA breaches involve "cyber threat indicators" under the Cybersecurity Information Sharing Act of 2015

# Phase 2 HIPAA Audits

- On July 11, 2016, The US Dept. of Health and Human Services Office for Civil Rights (OCR) began a second phase of audits of compliance with the HIPAA privacy, security, and breach notification rules
  - As required by the Health Information Technology for Economic and Clinical Health Act
  - 166 covered entities audited
    - 8.7% health plans, 1% healthcare clearinghouse, 90% provider
  - 41 business associates audited
- As expected, the Phase 2 covered entity audits focused on breach notification, as well as security risk analysis and management
- So far, OCR appears to be a tough grader, with many covered entities receiving the lowest scores of 4 or 5 out of 5

# Phase 1 Audit Findings

- More than 60% of the findings or observations were Security Rule violations
  - 58 of 59 audited healthcare provider covered entities had at least one Security Rule finding or observation
  - Even though the Security Rule represented only 28% of the total audit items
  - In Phase 1 audits, 2/3 of entities audited lacked a complete and accurate risk analysis
- Security Rule compliance is clearly a problem area

# Breach Lessons Learned from Phase 2 Audits

- OCR appears to be making fine distinctions when determining compliance deficiencies in the Phase 2 audits

- Covered entities have been cited for failure to use breach notification letters that meet all content requirements, including:
  - Recommendations for action the individual can take to protect against harm (such as information about reviewing credit reports)
  - A description of what is being done to investigate the breach
  - What is being done to mitigate harm to the individual
  - Actions to protect against future breaches

# Breach Lessons Learned from Phase 2 Audits (cont.)

- It is understandable that covered entities will be reluctant to
  - Provide details regarding an investigation
    - Because information can change quickly as the investigation unfolds
  - Provide details regarding mitigation efforts and actions to prevent incidents from recurring
    - Being too forthcoming can degrade security
  - Nevertheless, despite this reluctance, make sure that your breach notification letter says something that addresses each of the required informational elements
- Deficiencies cited in Phase 2 audits are likely to reappear in future OCR enforcement actions

# Preliminary Phase 2 Audit Findings

- In September 2017, Linda Sanches of OCR released preliminary results of the Phase 2 audits – and the results were not encouraging
- Timeliness of breach notification
  - 65% received best score of 1; 11% received worst score of 5
- Content of breach notification
  - 23% received score of 1; 7% received score of 5
- Content of Notice of Privacy Practices
  - 2% received score of 1; 15% received score of 5

# Preliminary Phase 2 Audit Findings (cont.)

- Provision of Notice of Privacy Practices
  - 57% received best score of 1; 15% received worst score of 5
- Right to access PHI
  - 1 received score of 1; 11 received score of 5
- Security risk analysis
  - Out of 63 covered entities, 36 received lowest scores of 4 or 5; none received a 1
- Security risk management
  - 46 out of 63 CEs received lowest scores of 4 or 5, one received a 1

# What's Next?

- Expect OCR to continue to focus future enforcement efforts on areas where systemic deficiencies have been identified
  - Security risk analysis
  - Security risk management
  - Content of breach notification

- "Phase 2 audits are about helping people comply, as opposed to freaking them out." Deven McGraw, OCR

- At 2017 AHIMA national conference in Los Angeles, Yun-Kyung "Peggy" Lee, deputy regional manager for OCR, announced that onsite audits would not take place in January 2018 as expected
  - OCR is reevaluating the audit program's approach and focus
  - Will probably be included in the next round of HIPAA audits

# WannaCry and NotPetya Malware

- Two major, global malware incidents grabbed headlines in 2017
- May 2017:  a WannaCry ransomware variant hit organizations around the world, including the UK's National Health Service
  - Initial reports suggested that US hospitals and healthcare organizations were not affected
  - However, follow-up attack in June 2017 did impact some US healthcare organizations
  - June 2017: OCR released email alerts stating that two large, multistate healthcare organizations were still struggling to recover from the impact of WannaCry
- June 2017 attack was NotPetya, a form of malware that masqueraded as ransomware but is actually designed to destroy data
  - Even if an organization did attempt to pay to regain access, the affected data was beyond recovery
  - Little official response by OCR to NotPetya

# HIPAA and Disaster Response

- OCR issued several guidance documents in 2017 in response to a series of natural disasters and high-profile emergency situations
  - Hurricanes Harvey, Irma and Maria
  - In response to these natural disasters, the following HIPAA requirements were waived on a temporary basis during the public health emergency
    - Distributing the Notice of Privacy Practices
    - Honoring a request to opt out of a facility directory
    - Obtaining the patient's agreement to disclose information to family members or friends involved in patient's care
    - Patient's right to request privacy restrictions and confidential communications

# HIPAA and Mass Shootings

- January 2017:  OCR issues updated guidance on permissible disclosures during emergency situations after December 2016 shootings at the Pulse nightclub in Orlando
  - Providers are permitted to disclose PHI to family members, friends, and other loved ones who are not married to the patient or otherwise recognized as relatives
  - Providers are not allowed to discriminate on the basis of sex or gender identity
- OCR reiterated and expanded on the hurricane disaster response guidance in October 2017 after the mass shooting in Las Vegas
  - OCR emphasizes that a formal HIPAA waiver is rarely required for an emergency situation like a mass shooting

# New OCR Web Tool on Breaches

- July 2017: OCR launches a revised HIPAA Breach Reporting Tool (HBRT) that helps individuals better identify recent HIPAA breaches and learn how breaches are investigated and resolved
- New features of the HBRT include
  - Enhanced functionality that highlights breaches currently under investigation and reported within the last 24 months
  - New archive that includes all older breaches and information about how breaches were resolved
  - Improved navigation to additional breach information
  - Tips for consumers

# Privacy Laws and Opioid Abuse Information

- October 27, 2017: OCR issues guidance on situations in which healthcare providers may share a patient's PHI with family members or friends when the patient may be in crisis and possibly incapacitated, such as following an opioid overdose
  - Issued the day after President Trump directed Acting HHS Secretary Eric Hargan to declare the opioid crisis a public health emergency
  - A few days later, on November 1, the president's Commission on Combating Drug Addiction and the Opioid Crisis issued its final report with 56 recommendations for responding to the opioid crisis
- Guidance does not address whether healthcare providers may report to law enforcement suspicions that a patient is diverting or selling prescription opioids or illicit drugs
  - Narrow HIPAA exception "in order to prevent or lessen a serious and imminent threat to the health or safety of a person or the public"

# OCR Responds to the Opioid Crisis

- December 18, 2017: OCR launches an array of new tools and initiatives in response to the opioid crisis
  - Also implementing the 21st Century Cures Act
- OCR seeks to ensure that patients and their family members can get the information they need to prevent and address emergency situations, such as an opioid overdose or mental health crisis
- Tools and initiatives also serve to ensure that the healthcare sector, researchers, patients, and their families understand how HIPAA protects privacy
- OCR's most comprehensive set of guidance documents focused on a single topic

# Example: HIPAA and Opioid Abuse Disclosures

- A 19-year-old adult patient who is addicted to opioids misses important medical appointments without any explanation
  - Parents are not "personal representatives" of the patient because patient is not a minor
  - Patient's PCP may believe there is an emergency related to the opioid addiction and may use professional judgment to determine that it is in patient's best interests to reach out to emergency contacts, such as parents or family, to inform them of situation
  - OCR guidance suggests that parents should establish themselves with child's provider as a helper or caregiver involved in care
  - PCP then knows not only whom to notify in an emergency, but also whom to call about their care
  - In cases involving significant impairment, parents may need to gain legal recognition as guardians or obtain a medical power of attorney to establish status as personal representatives
  - Remember that other federal and state laws may offer greater protections for substance abuse information

# OCR Responds to the Opioid Crisis

- OCR creates two new web pages focused on information related to mental and behavioral health, one for professionals and one for consumers
  - Guidance does not break new ground, but reorganizes existing guidance and provides a user-friendly, one-stop resource

- New collaboration with partner agencies within HHS to identify and develop model programs and materials for training healthcare providers, patients, and families regarding permitted uses and disclosures of PHI of patients seeking or undergoing mental health or substance use disorder treatment
  - Will be followed by outreach efforts to share the new programs and materials

# New Research Working Group

- OCR launches a new working group to study and report on the uses and disclosures of PHI for research purposes
  - Will include representatives from federal agencies, researchers, patients, healthcare providers, and experts in healthcare privacy, security, and technology
  - Will release a report addressing whether uses and disclosures for research purposes should be modified to facilitate research while protecting patient privacy rights

- Persistent concerns from the research community that the HIPAA Privacy Rule has created obstacles to clinical research

# New OCR Research Guidance

- Also in the December 18 publications, OCR issued new guidance on research, as called for in the 21st Century Cures Act
  - Also specific guidance sheet on uses of HIPAA authorizations for research
  - A research authorization need not describe each specific future study if the particular studies to be conducted are not yet determined. Instead, authorization must describe
    - Future purposes such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research
    - Example: Description could include specific statements with respect to whether sensitive research, such as genetic or mental health research, is contemplated
    - Privacy Rule does not prescribe a fixed level of detail about the future research or identify particular types of PHI as "sensitive"

# New Regulations on Substance Abuse Disorder Information

- January 3, 2018: The Substance Abuse and Mental Health Services Administration issues new rule updating the Confidentiality of Substance Use Disorder Records, 42 C.F.R. Part 2
  - Expands the circumstances under which substance abuse disorder (SUD) treatment providers may use and disclose to their third-party contractors individually identifiable information of patients receiving SUD treatment
  - Becomes effective on February 2, 2018
- Rule responds to a supplemental notice of proposed rulemaking issued in January 2017, seeking comment on certain issues

# Short-Form Redisclosure Notice

- 42 C.F.R. § 2.32 requires each disclosure of SUD information that is made with patient's written consent (i.e., a HIPAA authorization)
  - To include a four-sentence statement informing recipient of restrictions on further disclosure of the SUD information
- The Rule adopts an 80-character, abbreviated notice of the prohibition on redisclosure as a permitted option
- Short notice simply states:
  - "42 CFR part 2 prohibits unauthorized disclosure of these records"
  - Intended to make it easier for lawful holders who use EHR systems that impose character limits in free-text fields to send and receive the redisclosure notice

# SAMSHA's Balancing Act

- Amendments to Part 2 are intended to reconcile some of the tension between
  - HIPAA, which generally permits a wide range of information sharing of PHI for the benefit of ACOs, health information exchanges, and other innovative care models and
  - Part 2, which creates barriers to that sort of information-sharing with respect to SUD information
  - Remains to be seen whether new regulations will strike the right balance between protecting the privacy of this sensitive information and enabling legitimate uses by healthcare providers and exchanges

# Takeaways for Part 2 Programs

- Organizations that handle Part 2 information will need to
  - Update their patient consent forms to address release of SUD information for payment and healthcare operations purposes
  - Consider whether they wish to use the abbreviated notice regarding redisclosure in their authorization forms
  - Review relationships with subcontractors to determine what information may be shared with them
    - And amend or enter into contracts with subcontractors that meet new Part 2 requirements by the compliance date of February 2, 2020

# Upcoming OCR Regulations

- As stated by Deven McGraw at October 2017 Privacy + Security Forum
  - OCR will release an Advance Notice of Proposed Rulemaking on HIPAA whistleblower concept authorized by the HITECH Act
    - Will probably be issued sometime in 2018
    - "Advance" notice is significant and suggests a work-in-progress and significant industry input expected

- Accounting of disclosures regulation
  - Notice of Proposed Rulemaking issued in 2011 to implement HITECH Act provisions
  - Sought to expand accounting rights to reflect the capabilities of EHRs
  - Met with widespread criticism
  - Another Advance Notice of Proposed Rulemaking seeking industry input
  - Expected to be published in 2018

# Executive Order on Regulatory Cuts

- President Trump's January 2017 Executive Order mandates that two regulations be cut for every new regulation enacted
- OCR will need to grapple with the meaning of the Executive Order as new HIPAA regulations are introduced
  - What is the meaning of a "regulation"?
  - Obviously the HIPAA Privacy, Security, Breach Notification, Enforcement and Transactions and Code Sets Rules are not going to be cut in their entirety
  - Would "pruning" one of the less practical HIPAA Privacy Rule standards (accounting of disclosure, minimum necessary, business associate agreements) qualify as a regulatory cut?

# Further Out on the OCR Regulatory Horizon

- OCR is said to be working on the long-awaited guidance on the minimum necessary rule
  - Once again, based upon modifications authorized by the HITECH Act

- Will the business associate agreement requirements be eliminated?
  - Interestingly, Deven McGraw stated that BAAs are "a candidate for elimination"
  - Seems to recognize the amount of effort that the healthcare industry devotes to negotiating and entering into BAAs, even though business associates are legally required to adhere to the BA rules since the compliance date of the HIPAA Final Rule in September 2013
  - OCR is at least thinking about the appropriate regulatory posture for BAs as opposed to CEs
  - Don't get your hopes up

# Thanks!

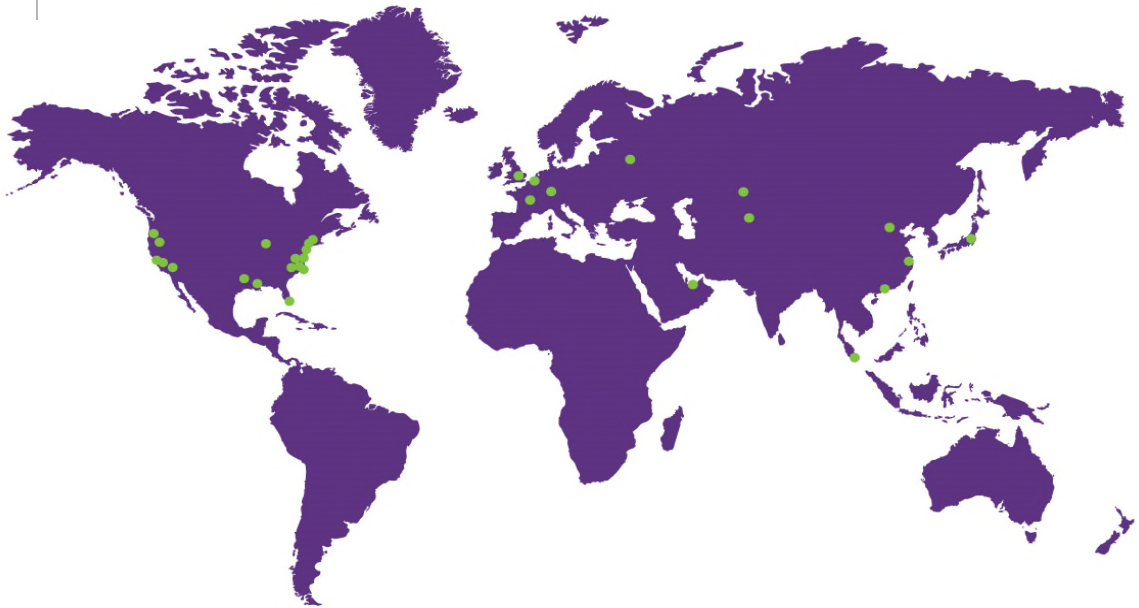
**Reece Hirsch**
Partner
Morgan Lewis
+1.415.442.1422
reece.hirsch@morganlewis.com

## 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.

# THANK YOU