
Morgan Lewis
NAVIGATING
THE NEXT.
Your IT Infrastructure and Systems – Cybersecurity and Data Privacy
Beth Herrington, Reece Hirsch, and Pulina Whitaker
June 3, 2021
© 2021 Morgan, Lewis & Bockius LLP

Presenters

Beth Herrington

Reece Hirsch

Pulina Whitaker

Morgan Lewis

Vaccine Information and Cybersecurity

- In the US, the recovery from the COVID-19 pandemic is in full swing
  - April 25: President of the European Commission said that Americans who have been fully vaccinated will be able to visit the European Union this summer

- Vaccine passports and other private initiatives will be a key component of the return to normalcy
- The Biden administration has declined to mandate vaccine passports or create a uniform system
  - Leaving it to state governments and the private sector to develop a variety of approaches
  - However, the federal government has indicated that it may play some role by offering guidelines on potential standardized proof-of-vaccine credentials

EU Digital Green Certificate Proposal

- A proposal was published earlier in April 2021 for an EU-wide framework for a Digital Green Certificate – it has gone live in 7 countries (Bulgaria, Croatia, the Czech Republic, Denmark, Germany, Greece, and Poland) ahead of a formal launch for the remaining 20 EU countries
- It is a QR code
- It would not restrict ability to travel – free movement across EU
- It is intended to facilitate travel
- NB – inadvertent or indirect discrimination will not be permitted by EU institutions
- Caution against creating two classes of citizens – those who have/have not had a COVID-19 vaccine
- The UK may sign-up to it but also has the NHS App now with a proof of COVID-19 status for travel feature

How Digital Green Certificate Works

- Issue of certificates (digital and paper) demonstrating:
  - Vaccinations
  - Test results
  - Recovery from COVID-19
- For third-country nationals staying in the EU during the pandemic – covers UK and US nationals or any other third-country nationals
- Principles of necessity and proportionality are key to implementation
- In February 2021, the European Council called for a common approach to vaccination certificates – not yet implemented; EU countries have taken individual approaches (e.g., Denmark)

European Privacy Framework

- GDPR and EU/UK privacy laws apply
- For EU Digital Green Certificate:
  - Proposal recommends issuing a list of who will be controllers (e.g., issuing authorities) and who will be processors (e.g., technology providers)
  - Technical and organisational measures to protect data are critical to data protection compliance – risk of a data breach would be a reportable high-risk incident
  - Transparency: privacy notice
  - Storage and retention of data: should be restricted to the purpose of the Certificate, with sunset clauses when pandemic ends
  - Privacy by design and privacy by default
  - Transfer of data across borders: needs to be lawful within the GDPR
- These issues apply to international vaccination passports – see Global Privacy Assembly statement: https://globalprivacyassembly.org/gpa-executive-committee-joint-statement-on-the-use-of-health-data-for-domestic-or-international-travel-purposes/

Other Vaccine Passport Options

- Airline apps (e.g., BA trial) or IATA Travel Pass
- Government mandates for disclosure of traveller data – can include testing data (depends on the airline)
- Privacy issues:
  - Who is controller
  - Transparency
  - Purpose limitation
  - Retention and storage limitations
  - Sunset deletion
  - Rights to control data
  - Privacy by design and by default

International Passports for Events

- There is no consensus for using passports for events or entry to bars and restaurants
- Israel recently dropped its plans for a passport
- The UK has said it has no plans for require or enable passports for entry to venues
  - We have had test events (e.g., The Brits and FA Cup Semi-Final)
  - So far, limited increase in infections from these events

HIPAA, FTC, and Vaccine Passports

- Vaccine passports raise one of the overarching themes in digital health privacy regulation – the overlapping jurisdiction of:
  - The Federal Trade Commission, the US privacy regulator with the broadest purview
  - The Dept. of Health and Human Services Office for Civil Rights (OCR), which enforces HIPAA
  - State Attorneys General
- OCR – regulates HIPAA covered entities
  - Healthcare providers that engage in standard electronic transactions
  - Health plans
  - Healthcare clearinghouses
- OCR also regulates business associates

PathCheck Foundation

- PathCheck Foundation at MIT is developing a "low-tech" vaccine passport program with Ideo
  - Uses a paper card, similar to what individuals receive after vaccination
  - To avoid fraud, the paper card would use multiple forms of verification, such as QR codes, for scanning
  - When scanned at a venue, card would only display individual's vaccination status
  - Other entities, such as healthcare providers, would be able to scan the card and access more detailed information
    - Type of vaccination received, date, location it was administered
- Reflects the notion that technology collecting consumer health information should be as minimal as possible to reduce privacy risks

Applying Privacy Best Practices

- Microsoft is partnering in the Vaccination Credential Initiative
  - Developing an "implementation guide detailing the use of open, interoperable, and privacy-protecting standards"
- The pandemic has raised unique privacy issues for companies, causing them to collect personal information from employees, such as temperature checks from visitors and travel histories from employees, that they hadn't previously collected
- Traditional privacy law principles have still been sufficient to address these new issues
- Same appears true of vaccine passports
  - Rely on traditional privacy best practices such as transparency, purpose limitation, and data minimization

When Are Vaccination Records Subject to HIPAA?

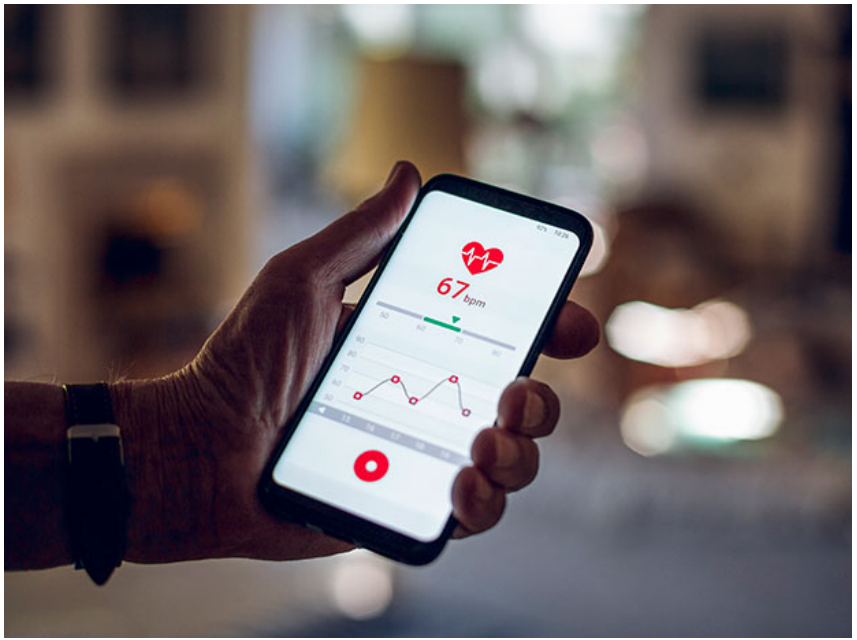
- A provider administering COVID-19 vaccinations may or may not be a HIPAA covered entity
  - In order to be a HIPAA healthcare provider covered entity, the provider must
    - Provide "health care" (very broadly defined) AND
    - Engage in HIPAA standard electronic transactions (which essentially means electronically billing payors for healthcare services)
- Let's assume that a COVID-19 vaccine is administered by a HIPAA covered entity, such as a hospital or pharmacy
- The vaccination record can only be disclosed by the healthcare provider to a vaccine passport company in accordance with HIPAA privacy and security rules

The FTC and OCR

- 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 first used the "unfairness document" 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 amounts of health information that consumers are sharing through mobile apps, wearable devices, personal health records, and now vaccine passports, referred to as consumer-generated health information (CHI)
- May 2014: FTC conducts a seminar titled "Consumer Generated and Controlled Health Data"
- April 2016: FTC, in conjunction with OCR and FDA, releases the "Mobile Health Apps Interactive Tool"
- October 2016: FTC and OCR put out business guidance titled "Sharing Health Information? Look to HIPAA and the FTC Act"



FTC Security Program Guidance

- Recent FTC settlements have required comprehensive information security programs that typically include these elements:

1) Appoint one or more employees responsible for the program
2) Identify internal and external risks to personal information (recent settlements have required that self-assessments be conducted at least annually and following a breach)
3) Design, implement, test, and monitor the effectiveness of the safeguards that address risk
4) Retain service providers capable of protecting personal information

FTC Security Program Guidance (cont.)

5) Evaluate and adjust the program as necessary (recent settlements have required evaluation and adjustment at least annually or after changes to the business or a breach)
6) Retain independent third-party assessors to evaluate the effectiveness of the program (at the time of the settlement and biennially thereafter)
7) Document the relevant internal and external risks and the relevant safeguards
8) Document the "content, implementation, and maintenance of the program"

Applying HIPAA Security Standards

- The cornerstone of HIPAA Security Rule compliance is the risk analysis
  - "An accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI"
    - 45 CFR § 164.308(a)(1)(ii)(A)

HHS Cybersecurity Report "Micro" Steps

- In June 2017, an HHS task force issued its Report on Improving Cybersecurity in the Health Care Industry
  - "Health care cybersecurity is in critical condition"
- Recommended immediate "micro" steps
  - Allocating time and resources to get the most protection efficiently
  - Developing a data map and device inventory to identify sensitive electronic information
  - Performing a data classification exercise to determine the number and types of security controls appropriate to safeguard data
  - Conducting and implementing a risk analysis
  - Developing a risk management plan
  - Managing residual risk (after security measures have been applied)
  - Reviewing vendor contracts with an eye to risk management
  - Evaluating cyberliability insurance

HHS Cybersecurity Report "Macro" Steps

- Develop the workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
- Increase organizational readiness through improved cybersecurity awareness and education
- Identify mechanisms to protect research and development efforts, and intellectual property, from attacks or exposure
- Improve information sharing regarding industry threats, risks, and mitigations

HIPAA Privacy: Authorization or Access Request?

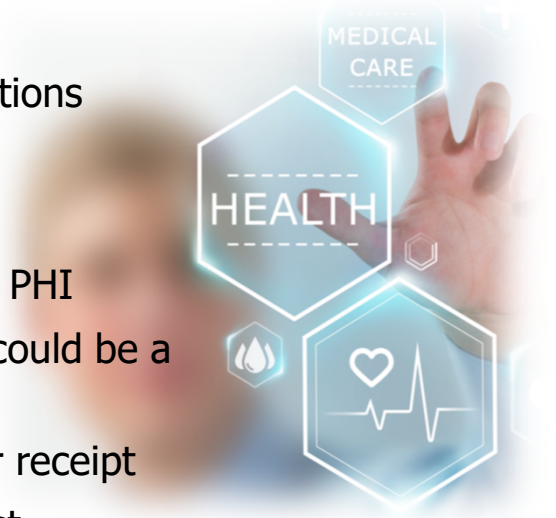
- HIPAA does not appear to include an exception for disclosure of protected health information (PHI) that would apply to vaccine passport programs
- Therefore, the disclosure must be pursuant to:
  - A HIPAA authorization executed by the individual
  - A HIPAA access request by the individual
- Paths are similar but have differing characteristics

HIPAA Authorization

- Key characteristics of a HIPAA authorization
  - Permits, but does not require, a covered entity to disclose PHI
  - Requires a number of specific provisions
  - No timeliness requirement for disclosing PHI
  - Reasonable safeguards apply (PHI must be sent securely)
  - No limitation on fees that may be charged to the person requesting PHI
    - But electronic transfer of vaccination records may not entail significant costs for the covered entity
- HIPAA authorizations may be executed online with an electronic signature

Patient Access Request

- Key characteristics of a HIPAA patient access request
  - Covered entity is required to disclose PHI, subject to limited exceptions
  - Must be in writing
  - Signed by the individual (can be an electronic signature)
  - Must clearly identify the designated person and where to send the PHI
    - The individual can designate a recipient of the access request (could be a vaccine passport company)
  - Covered entity must act on the request no later than 30 days after receipt
  - Reasonable security safeguards apply, but an individual can request transmission by unsecure medium (such as unencrypted email)
  - Fees charged by covered entities are limited (but limitation does not apply to disclosures to a third party, such as a vaccine passport company)



Authorization or Access Request?

- Access requests have certain advantages
  - Shorter document
  - Covered entity required to respond
  - Covered entity must respond within a required time frame (30 days)
- However, a vaccine passport company would need to be clearly authorized by the individual to submit the access request on the individual's behalf
  - Could be accomplished through the Terms of Service, but must be very clear because it's essentially an agency appointment
- Arguably, HIPAA authorizations are more commonplace and better understood by covered entities compared with access requests to designated third parties

How Much Information to Request?

- A HIPAA authorization must specify the PHI to be disclosed
- A HIPAA access request could include the entire "designated record set" maintained by the covered entity, but may also be limited to specific information
- Data minimization is a general privacy best practice
  - Requesting robust medical information beyond the vaccination record and related demographic information increases privacy risks
  - The more medical information collected, the greater the risk in the event of a security breach
  - A major security breach could damage confidence in a vaccine passport program and perhaps in vaccinations in general

Is a Vaccine Passport Program a PHR?

- What is a Personal Health Record (PHR)?
- No universally accepted definition
  - 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"
- Vaccine passport programs can take on characteristics of a PHR depending on the amount and type of CHI collected
- Distinct from an electronic medical record (EMR), which is maintained and largely controlled by a healthcare provider

FTC's Health Breach Notification Rule

- If a vaccine passport program is a PHR, then it may be subject to FTC's Health Breach Notification Rule
  - 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
- May 2020: FTC seeks comments on the Rule, including whether it should be applied to health apps, virtual assistants, and platforms' health tools

Incident Response Plans

- Documenting and implementing a comprehensive incident response plan is one of the best things that an organization can do to reduce cybersecurity risk
  - Mitigates substantial damages that may arise from a significant and poorly managed breach
  - A security breach involving vaccination records could jeopardize consumer confidence in vaccination records or passport programs

Incident Response Plan Is an Enterprise-Wide Document

- A key component of a security compliance program is an incident response plan
- Often developed as a stand-alone module distinct from security policies and procedures
  - More than just a technical systems document; requires input from legal, compliance, and others
  - Includes employee-facing components

Security Breaches Involving Vaccination Records

- Security breaches pose the single greatest privacy and security regulatory risk for healthcare organizations
  - Often leads to OCR or state attorney general investigations
  - Prompts regulators to examine an organization's overall security compliance program
- A security breach is not necessarily evidence that an organization's security measures are deficient – current cyber threats are sophisticated, and no organization is immune
- Failure to implement an appropriate security incident response plan IS a sign of an inadequate approach to cybersecurity, and in some instances it's a violation of legal standards
- A thoughtful, documented, battle-tested incident response plan is the best way to mitigate reputational harm and defuse regulatory scrutiny related to a breach

Takeaways

- Vaccine passport programs and other private vaccination initiatives pose unique cybersecurity, privacy, societal, and ethical concerns
- All the more reason for passport programs (and the businesses and employers that utilize them) to consider the FTC's mantras of privacy by design and security by design
  - Baking in privacy and security during the development of a product or service
- As with other digital health products, it's also critical to be aware of where the regulatory lines are drawn in the overlapping authority of
  - OCR
  - FTC
  - State Attorneys General

Litigation Avoidance in Dynamic Area of Law

- Dynamic, fast-moving area of the law
  - State governments likely will lead variety of approaches and laws
- Federal guidance from EEOC
  - Vaccination status surveys from federal law, specifically ADA
- State omnibus data privacy laws
  - California Consumer Privacy Act (CCPA)
  - Virginia data privacy law effective January 1, 2023

State Omnibus Data Privacy Laws

- Data privacy laws applicable to company's data, including employees' vaccination status
- CCPA requires notice before collection, even if employers are located out of state
- Pending legislation in numerous states
  - Florida & Texas: moved to ban requiring proof of vaccination to take part in everyday activities

State Data Security and Data Breach Laws

- Laws that require employers to "take reasonable steps" to secure "personal information" (most states)
  - Illinois
- Laws that create liability shield in the event of a data breach if the employer stores "personal information" in statutorily prescribed ways
  - Ohio
- All states have data breach notification laws
  - Must follow specified notification procedures if "personal information" is exposed by a data breach
  - Vaccination status can be "personal information"

.

New and Existing State Employment Laws

- May impose requirements on employers seeking their employees' vaccination status
- Types of laws fall into two categories:
  - Pre-existing employment laws that happen to apply to vaccination status data collection or retention
  - States considering legislation that restricts private businesses from asking their employees for proof of vaccination or abut their vaccination status
    - Illinois (HB 3862)
    - New York (AB 4602)

Litigation Avoidance Strategies

(1) Work with counsel to verify which state data privacy laws or data security/notification laws with which your company must comply

- Does vaccination status data constitute "personal information" under any applicable law?

(2) Prepare to store vaccination status data as you would Social Security Numbers, driver's license numbers or other PII

(3) Ensure any employee survey avoids inquiring further if employee says they are not getting the vaccine

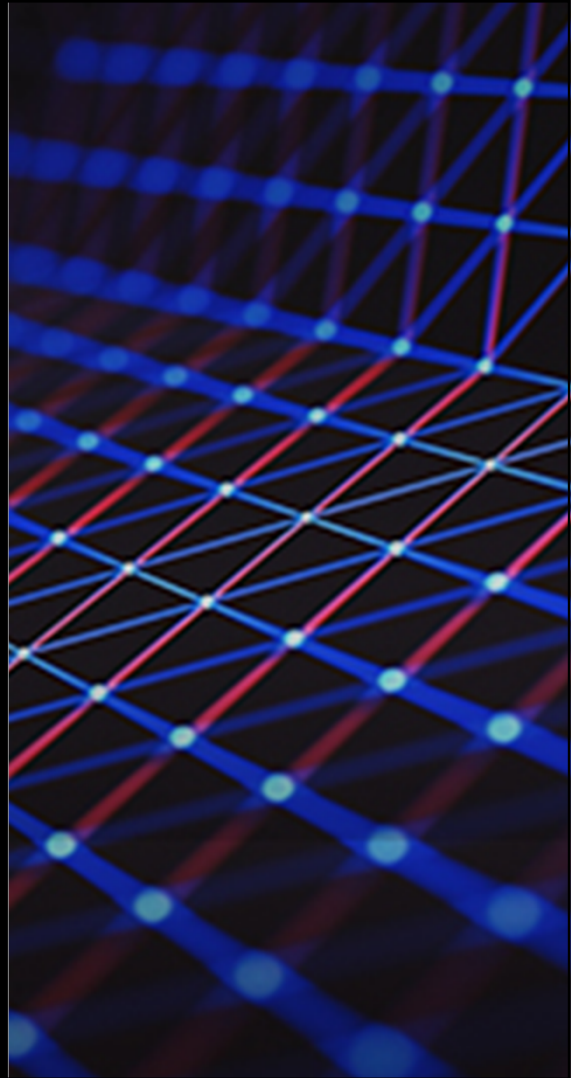
(4) Keep an eye on growing enacted and pending legislation

Coronavirus/ COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at **www.morganlewis.com/topics/coronavirus-covid-19**

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to **subscribe** using the purple "Stay Up to Date" button.



Morgan Lewis

Elizabeth B. Herrington

Partner
Morgan, Lewis & Bockius LLP
Chicago
beth.herrington@
morganlewis.com
+1.312.324.1445

Elizabeth ("Beth") Herrington focuses her practice on complex commercial and class action litigation across the United States, including management of multi-jurisdictional related investigations and litigation. Many challenges facing companies today present multiple dimensions and Beth works with companies to shape overall strategy to successfully navigate these challenges. Beth regularly represents domestic and international retail/eCommerce companies, technology and mobility companies, consumer service providers, and product manufacturers in high-exposure investigations and lawsuits that involve fraud, privacy claims, tax, and trade secret theft.

Education

University of Illinois College of Law, 1997, J.D., Cum Laude
Miami University, 1994, B.A., Cum Laude

W. Reece Hirsch

Partner
Morgan, Lewis & Bockius LLP
San Francisco
reece.hirsch@
morganlewis.com
+1.415.442.1422

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."

Education

University of Southern California Law School, 1990, J.D.
Northwestern University, 1982, B.S.

Pulina Whitaker

Partner
Morgan, Lewis & Bockius LLP
London
pulina.whitaker@
morganlewis.com
+44.20.3201.5550

Pulina Whitaker's practice encompasses data privacy and cybersecurity as well as employment matters. Co-head of the firm's global privacy and cybersecurity practice, she manages employment and data privacy issues on an advisory basis and in sales and acquisitions, commercial outsourcings, and restructurings. Pulina manages international employee misconduct investigations as well as cross-border data breach investigations. She has been appointed as a compliance monitor for the United Nations and for USAID. She is also a trustee of Hostage International.

Education

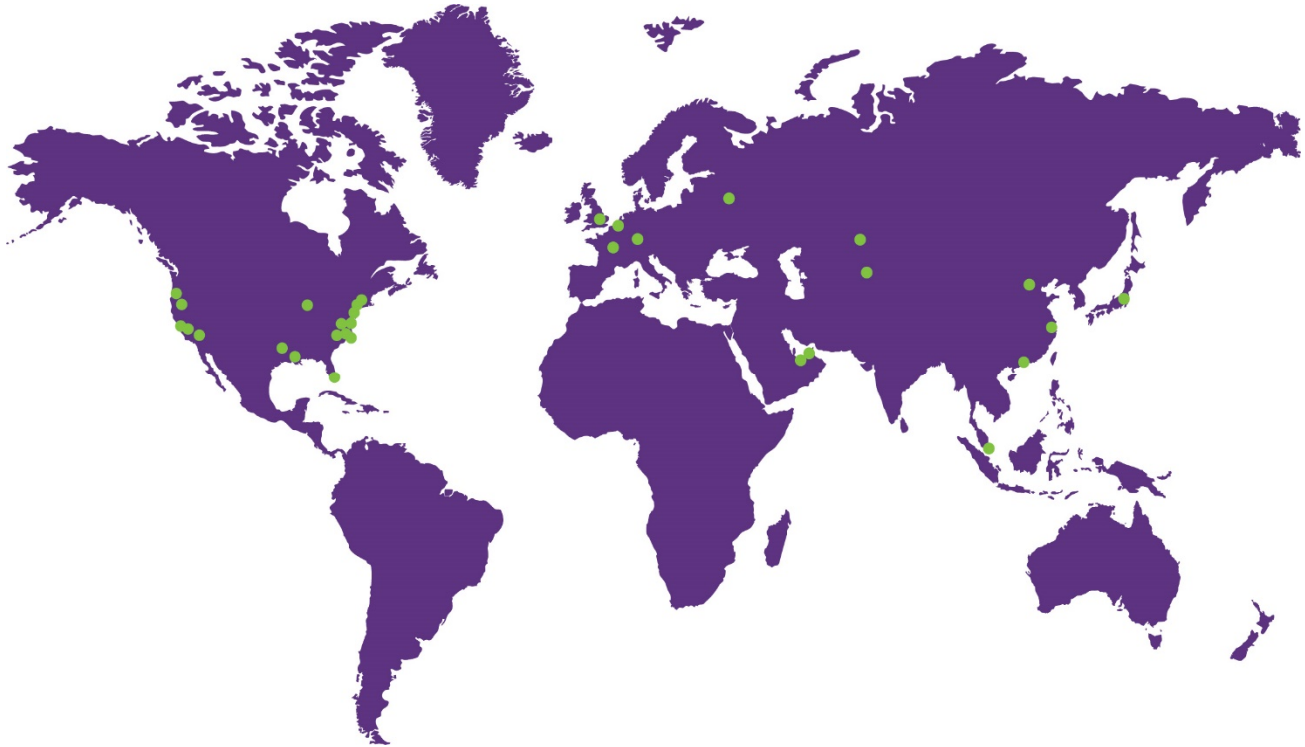
College of Law of England and Wales, Chester, 1997, LPC
University of Bristol, England, 1996, LLB, with Honors

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



Morgan Lewis

THANK YOU