

Morgan Lewis

NAVIGATING THE NEXT.

Digital Vaccine Passports

Reece Hirsch and Pulina Whitaker

April 29, 2021

Presenters



W. Reece Hirsch



Pulina Whitaker

Morgan Lewis

Vaccine Passports: US Privacy Issues

The background of the slide is a composite image. At the top, there is a dark blue space filled with stars and a glowing horizon line. Below this, a cityscape is visible at night, with buildings and streets illuminated. Overlaid on the cityscape is a network of glowing blue lines and dots, resembling a data network or a globe's connectivity. The overall color palette is dominated by blues, oranges, and whites.

Morgan Lewis

Vaccine Passports: The Time Has Come

- In the US, the recovery from the COVID-19 pandemic is in full swing
 - Approximately 29% of Americans are now fully vaccinated
 - 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 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



A Variety of Approaches

- Because there will not be a single US vaccine passport standard, each developer of a program may weigh privacy, societal, and ethical concerns differently
- And some states may resist the idea of vaccine passports entirely
 - Florida and Texas have moved to ban requiring proof of vaccination to take part in everyday events, such as attending sporting events, restaurants, and movie theaters
 - Florida Governor Ron DeSantis: Vaccine passports “would create two classes of citizens based on vaccination” and threaten individual freedoms, health privacy, and the free flow of commerce

New York's Excelsior Pass

- In March, New York was the first state to launch a vaccine passport program, the Excelsior Pass
 - A free, voluntary platform
 - Developed in partnership with IBM
- Allows consumers to store proof of their vaccination or negative test results on their phones through a secure QR code
- Participating businesses and venues, including Madison Square Garden and Albany's Times Union Center, can scan using a companion app
- Because the pass uses an encrypted digital wallet on a smartphone to store the information, organizations will be able to verify credentials without having access to individuals' underlying personal data
- Use of blockchain technology eliminates the need for a central database, creating a "hash" of data used for verification



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



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



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"



HIPAA, FTC, and Vaccine Passports

- 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 rules

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 the PHI
 - Reasonable safeguards apply (PHI must be sent securely)
 - No limitation on fees that may be charged to the person requesting the 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 timeframe (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 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

Privacy Laws Applicable to Vaccine Passport Companies

- A vaccine passport program will generally be consumer-directed
 - Would not be a HIPAA business associate because “acting on behalf of” the individual, not on behalf of a HIPAA covered entity
 - Would typically be subject to
 - FTC privacy and security principles
 - State Attorney General privacy enforcement under “Baby FTC Acts”
 - State security breach notification laws
 - Some states, such as California, define “personal information” to include name plus “medical information”



California Consumer Privacy Act (CCPA)

- Vaccine passport programs that operate in California and are consumer-directed will likely be subject to the landmark California privacy law
 - Will likely not qualify for CCPA's exception for HIPAA regulated entities and PHI
- In 2023, California Privacy Rights Act (CPRA) will become effective, enhancing CCPA
 - Will permit consumers to opt out of a business's use and disclosure of "sensitive personal information"
 - Includes health and biometric information
- CPRA also includes a proportionality standard that incorporates the data minimization concept

Virginia Consumer Data Protection Act

- Effective on January 1, 2023
- Similar to the CCPA, as enhanced by the CPRA
- One notable difference – businesses must obtain express “opt in” consent from consumers when the business
 - Processes sensitive data or
 - Deviates from the purposes disclosed in the business’s privacy policy
- “Sensitive data” includes “mental or physical health diagnosis,” “biometric data,” and “precise geolocation data”

Takeaways

- Vaccine passport programs pose unique 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

European Privacy Issues

The background of the slide is a composite image. At the top, a bright sun or star is on the horizon, casting a glow over a dark, starry space. Below this, a network of glowing blue lines connects various points, resembling a global communication or data network. The bottom half of the image shows a night view of a city with illuminated buildings and streets, overlaid with the same network of glowing blue lines.

Morgan Lewis

EU Digital Green Certificate Proposal

- A proposal was published earlier in April 2021 for an EU-wide framework for a Digital Green Certificate
- 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
- What will the UK do?

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
- 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 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
- 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



W. Reece Hirsch



Partner
Morgan, Lewis & Bockius LLP
San Francisco
[reece.hirsch@
morganlewis.com](mailto: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](mailto: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

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.

Morgan Lewis

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](http://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.

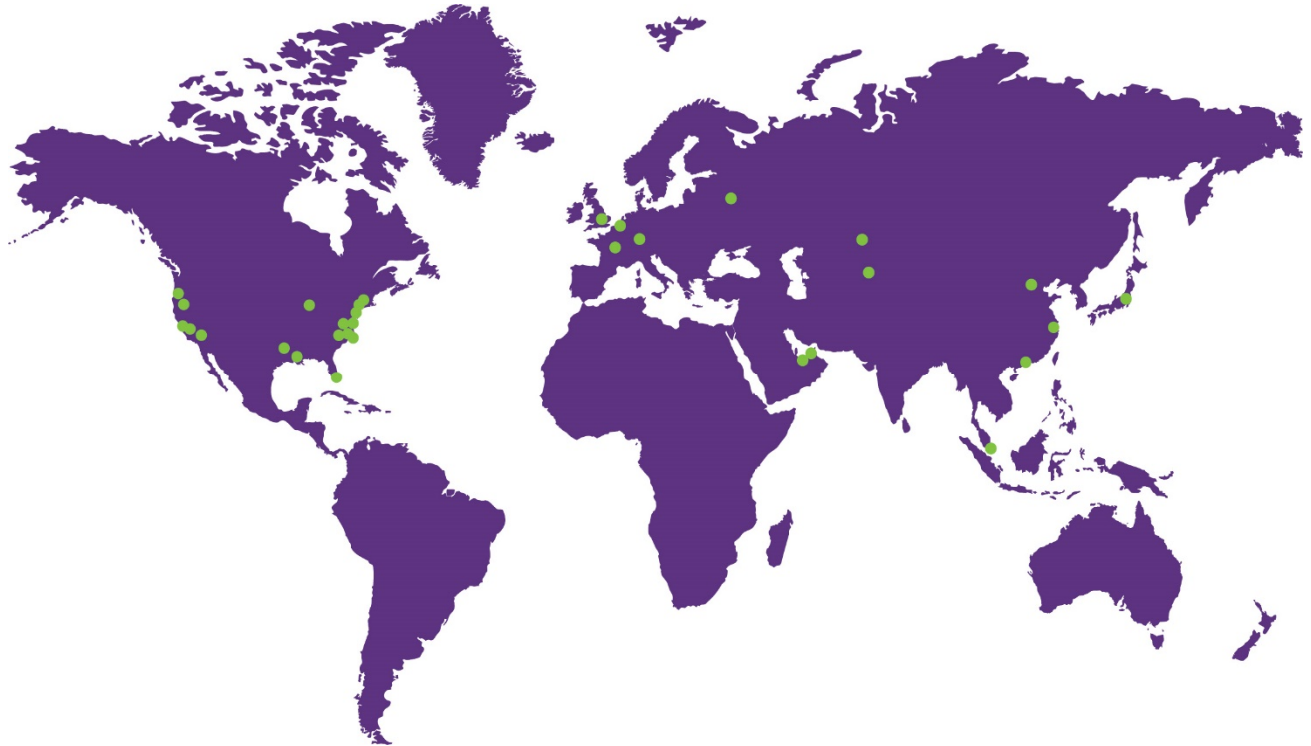


Our Global Reach

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

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

© 2021 Morgan, Lewis & Bockius LLP
© 2021 Morgan Lewis Stamford LLC
© 2021 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.