Fox Rothschild LLP
ATTORNEYS AT LAW

Publications

Future Imperfect: Vaccine Passports Pose Complex Privacy Questions

May 19, 2021 – Alerts
by Mark G. McCreary

Multiple times a day, clients ask us whether vaccine passports will be the admission ticket to the post-COVID-19 future. For many events and travel in many jurisdictions, the answer is likely yes. But what does that mean for businesses?

Vaccine passports are paper or digital forms certifying that a person has been vaccinated against a disease. Here we are discussing digital certifications, most likely on a mobile device, confirming that an individual has been fully vaccinated against COVID-19.

If a business is considering utilizing vaccination passports, it should be asking these questions:

- What do we need to know in order to comply with state, federal or international laws when collecting, maintaining, processing or even sharing individuals' vaccine passport information?
- What technical measures should be in place to ensure the security of the information?
- Should we use a vendor? If so, how do we know the vendor is complying with relevant privacy and data security laws and regulations?
- Is our business in an industry that is more likely to benefit from a vaccine passport, such as commercial air travel, child care, higher education, hotels, live performance venues and restaurants?

Fox Rothschild's Privacy & Data Security attorneys have been investigating these and other related questions and helping clients navigate these difficult waters. Here are some practical answers to common questions about the business, privacy and risk issues surrounding the use of vaccine passports.

Initial Legal Questions

Like nearly everything COVID-19-related, the use of vaccine passports differs based on geography. Some states are allowing or even facilitating the use of such tools by the private sector. For example, Hawaii is working on creating a vaccination verification process and New York already has an option available, discussed in detail below. On the other end of the spectrum, several states such as Arizona, Florida, Idaho, Montana, Texas and Utah have banned local governments or businesses from requiring patrons to provide proof of vaccination for everyday activities such as visiting bars, restaurants and movie theaters, attending sporting events and boarding commercial flights. Explaining his state's ban, Florida Gov. Ron DeSantis said that requiring proof of vaccination status "would create two classes of citizens based on vaccination" and threaten individual freedoms, health privacy and the free flow of commerce.

Because there is so much variation, businesses should stay abreast of vaccination passport laws and regulations in all states in which they operate.

Limiting Data Collected and Data Sharing

ASSOCIATED PEOPLE

- Mark G. McCreary, CIPP/US

ASSOCIATED PRACTICES

- Privacy & Data Security
- California Consumer Privacy Act
- GDPR Compliance & International Privacy

Whether employing vaccine passports voluntarily or in response to government mandates, businesses' first and most important objective will be to **limit the amount of data collected**. As has become commonplace through new laws in force in both Europe and the United States, **Data Minimization** is the best approach — that is, only collect the information that is necessary to accomplish your purpose.

Determining the minimum data necessary to verify an individual's vaccine status will depend on the business and the purpose of determining the person's vaccination status. Airlines, concert venues, restaurants and sports venues likely only need to know whether or not an individual is vaccinated. Arguably, health care-related entities such as hospitals and vaccination sites could benefit from knowing more about the individual, such as the date and location of vaccination, their ethnicity and underlying health conditions. But for most vaccine passport uses, it will not be necessary or advisable to collect this additional information or geolocation tracking information.

The second central objective will be to **limit or prohibit the subsequent disclosure of that collected data**. Privacy advocates argue that to maintain confidentiality and public confidence, the data collected for vaccine passports should never be aggregated to establish a central database of consumer data. The data collected should be limited to that necessary to accomplish the purpose – allowing the individual to provide proof of vaccination so that he or she may be allowed admission or to travel.

Few business owners need to know anything more than whether an individual is fully vaccinated. It is difficult to make a convincing argument that a business needs to know when or where an individual was vaccinated, or whether that person had previously been infected with COVID-19 or has any underlying medical conditions.

Selection of Vaccine Passport Solution Vendors

Once a business has determined what data it will collect and with whom that data will be shared, it can begin searching for a vendor that meets its needs.

Businesses should look for a vendor that practices **Privacy by Design**, a concept that has become mainstream with the European Union's General Data Protection Regulation (GDPR) and new U.S. state privacy laws. Put simply, Privacy by Design is an approach that ensures businesses consider privacy and data protection issues at the design phase and throughout the lifecycle of any system, service, product or process.

Beginning with the vaccine passport data collection and retention system, the business should ask whether the vendor has designed its product to collect only the data that the business has determined is necessary and to restrict unnecessary, further disclosure of that data? In other words, is the vendor using a Privacy by Design approach in building its vaccine passport product?

We believe that a deliberate and thoughtful Privacy by Design approach is critical for the success of any vaccine passport product in the United States.

Disclosure and Consent

As with all things privacy related, businesses must disclose their data collection, monitoring and usage practices. Consumers must be clearly informed about what data is being collected, how they are being monitored and how their data will be used so they can choose whether to allow such collection, monitoring and usage.

Consumers must be permitted to actively choose to allow such collection, monitoring and usage. Simply disclosing the process of such data collection, monitoring and usage without obtaining explicit consent from the consumer is inadequate. A business should seek consent from individuals through a means that requires them to take active steps to affirm their permission. That can be as simple as providing an opportunity to review a properly drafted Privacy Notice that describes (among other things) what data is collected, how it is used and to whom it will be disclosed, and requiring them to check a box (that is not presented as checked) acknowledging their consent.

Security

The privacy and security worlds are quickly merging, and a vaccine passport is an excellent example of where that occurs. Ideally, the passport vendor should never receive any of the data

entered by the individual. That information could continue to reside on the smartphone, for example. However, not all solutions will offer that approach, and that is not necessarily a problem. In fact, if it is a state-provided solution, the government may already have the same information from a consumer's testing and vaccination records.

It is an absolute requirement that the provider of any vaccine passport solution that collects personal information take "**adequate technical and organizational measures**" to secure this data. There are many ways to address appropriate security and there is not a one-size-fits-all answer. However, what is required is likely more than what you expect, and that bar continues to be raised.

Collection of Sensitive Data

Businesses and government should also understand the legal significance of the information that is being collected. The GDPR, which has been in effect since 2018, as well as the California Privacy Rights Act and Virginia Consumer Data Protection Act, which are both set to go live in 2023, include **heightened protections for "sensitive" consumer data**, a category that includes health and location information that may find its way into at least some versions of vaccine passports.

The new California privacy law expands the state's landmark Consumer Privacy Act by giving consumers the right to limit the use and disclosure of a new category of "sensitive" personal information, while the Virginia law is the first in the nation to require companies to obtain affirmative opt-in consent for processing sensitive data. Both states include health information, race, ethnicity and precise geolocation data in their definitions of "sensitive" data.

New York's Solution

New York launched its vaccine passport solution, dubbed Excelsior Pass, in March. Developed with IBM, this solution is being used to replace vaccination cards and COVID test results. Excelsior Pass can already be used at many venues, including Yankee Stadium and Madison Square Garden, and is intended to eliminate the need for an individual to carry a CDC vaccination card or evidence of a recent negative COVID test.

The benefit of Excelsior Pass, like a well-implemented vaccine passport, is that a business can verify the vaccination status of an individual without the individual sharing any further information with the business. All the business sees is a QR code that, when scanned, indicates that the individual is vaccinated.

Excelsior Pass has some critics. Some complain that this information is being shared with the state of New York, which is inherently dangerous because of state governments' long record of inadequate data protection. It should be noted, however, that the information required to be provided to the state of New York in connection with Excelsior Pass is information that the state already has.

Additionally, there is little to stop an individual from sharing their QR code with others. Most vaccine passport solutions will depend somewhat on the honor code, although it is imaginable that vendors will devise creative ways to ensure the individual presenting the QR code is who they say they are.

Florida's Ban on Vaccine Passports

Florida has taken the opposite approach to New York and has prohibited any use of vaccine passports, citing concerns that they promote discrimination against non-vaccinated individuals. Florida is concerned that "use of vaccine credentials raises concerns that unvaccinated individuals could be treated unfairly by employers, businesses, governmental entities or the community at large."

Before a business adopts a vaccine passport verification process, it is important to consider the web of local, state, federal, and international privacy and data security laws that may be implicated by this process.

For more information, please contact Privacy & Data Security Practice Co-Chair Mark McCreary, CIPP/US at 215.299.2010 or mmccreary@foxrothschild.com.