Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Vaccine Passport Plans Can't Ignore Web Of Privacy Laws

By **Allison Grande**

Law360 (April 22, 2021, 10:12 PM EDT) -- As governments and businesses increasingly consider instituting systems to check whether travelers and eventgoers have received COVID-19 vaccines, they'll need to pay careful attention to an emerging global patchwork of privacy laws that will likely limit what's in these so-called vaccine passports.

After more than a year of grappling with thorny questions about how to legally and ethically track the spread of COVID-19, governments' and companies' attention now turns to efforts to verify whether individuals who want to travel, attend an event or engage in other public activities have been vaccinated.

The vaccine passports that will be used for this verification, like the Excelsior Pass developed by IBM that was recently rolled out in New York state, raise a host of data privacy and security issues that regulators, including the European Union's national data protection authorities, have already indicated they'll be watching carefully.

"The experience of the past year shows that data protection does not get in the way of solving practical problems like fighting the pandemic and helping us exit it, but it is important to do that within the applicable legal framework around privacy and cybersecurity," said Eduardo Ustaran, who's based in London and serves as global co-head of the privacy and cybersecurity practice at Hogan Lovells.

"The right privacy practices can make a significant contribution to the lawful and ethical rollout of vaccine passports," Ustaran said. "Well-accepted principles like transparency, purpose limitation and data minimization can guide this deployment, and practical tools like privacy impact assessments will ensure that we achieve the best of all possible worlds."

The pandemic has thrust many companies into novel waters, pushing them to gather personal information such as temperature checks from visitors and travel histories from employees that they wouldn't normally collect. Asking people to show proof that they've received a COVID-19 vaccine in exchange for entry on a plane or into a venue presents the same type of privacy and data security concerns and should be treated in a similar way, experts say.

"The key when reviewing these types of systems is to consider, are they designed to limit the amount of personal data that they collect and the amount of personal data that gets disclosed in their use," said Alan Butler, executive director and president of the Electronic Privacy Information Center.

Health care providers that administer the vaccine need to follow the privacy and data security rules laid out in the Health Insurance Portability and Accountability Act when gathering personal data, but airlines, sports teams and other private businesses that may want to set up ways to check vaccine statuses won't be bound by these rules.

Instead, they'll need to consider frameworks that are being implemented around the world that are designed to give consumers more control over how companies use and share their data, including new laws in California and Virginia and the EU's General Data Protection Regulation.

Specifically, businesses need to ensure that they have consent to use the data they're collecting, that they're not using this information for purposes beyond the reason it was collected, and that they're safely and securely storing this data, said Catherine Zhu, special counsel at Foley & Lardner LLP.

"The last thing a company would want is a data breach of all this vaccine data," Zhu said. "Not only could that result in regulatory penalties, but it would also undermine public trust and the whole optics of vaccine passport use."

The European Data Protection Board, which is made up of national data protection regulators from each EU member state, stressed these principles in an April 6 opinion on efforts to develop so-called digital green certificates to aid reopening efforts. The European Commission has proposed establishing a common framework for such certificates, which could be used to verify COVID-19 vaccinations, test results or people's recovery from the disease.

The regulators stressed that the use of these certificates must be "fully in line with the fundamental principles of necessity, proportionality and effectiveness" that are core to the GDPR. They welcomed the commission's proposal that the certificates should contain "only the personal data necessary for the purpose of facilitating the exercise of the right to the free movement" within the EU during the pandemic, while warning that these certificates should never be combined to create a central database of consumer data.

The data protection authorities also advised that, in order to comply with the GDPR, companies would need to take "adequate technical and organizational measures" to secure this data, ensure that individuals are not discriminated against based on their health status and agree that they would stop using the data once the pandemic has subsided.

"I have always stressed that measures taken in the fight against COVID-19 are temporary and it is our duty to ensure that they are not here to stay after the crisis," European Data Protection Supervisor Wojciech Wiewiórowski said in a statement accompanying the opinion.

Given this input, deciding what data is actually necessary in order to verify someone's vaccine status will need to be a key consideration for companies and governments that want to develop and make use of these credentials, attorneys say.

"Understanding the intended use before the data is collected enables decisions to collect the least information necessary," said Jodi Daniel, a partner at Crowell & Moring LLP.

For example, vaccine sites may ask people for information about underlying health conditions or race and ethnicity, and those that are developing apps and other ways to keep tabs on vaccine statuses may

be able to track locations when a credential is accessed, according to Daniel. However, "such information may not be necessary if the goal is simply to have a record of vaccine status, and additional data raises increased privacy and security risks," Daniel said.

Still, while companies will likely want to err on the side of minimization, the unprecedented nature of the pandemic is likely to complicate the question of what information may be necessary to collect and retain in the long term.

"The general rule from a privacy perspective is that the extent you can do something with less information, that's usually better," said Jennifer Geetter, a partner at McDermott Will & Emery LLP. "But that can be difficult when you're at the outset of something like this, when you're trying to figure out what you need to know to best protect the community and you can't always anticipate the information that you may need to do that."

The nature of the data that companies collect may also affect what regulations come into play.

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 handing 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.

"Companies need to be thinking about whether they're collecting not personally identifiable information but also sensitive personal information, and what they'll need to do in that situation," said Zhu, the Foley & Larder attorney.

Additionally, ensuring that consumers are clearly informed about what data's being collected and how it's used, and allowing them to choose whether they want to participate in these efforts at all, will go a long way toward complying with applicable legal frameworks in both the U.S. and abroad, attorneys say.

New York appeared to have these issues in mind last month when it became the first state to formally launch "this potentially transformational technology" in the form of the Excelsior Pass, a free, voluntary platform developed in partnership with IBM that New Yorkers will have to opt in to use.

The digital health pass allows consumers to store proof of their vaccination or negative test results on their phones through a secure QR code that participating businesses and venues, including Madison Square Garden and the Times Union Center, can scan using a companion app. Because the pass uses an encrypted digital wallet on a smartphone to store this information, organizations will be able to verify these credentials without having access to individuals' underlying personal data, putting consumers in charge of what information they share, the state and IBM said.

Butler, EPIC's president and executive director, said the New York system appeared to be on the right track, given officials' statements that the Excelsior pass only communicates whether a person has satisfied the requirements of being vaccinated and doesn't create a permanent log of individuals'

vaccine status or where they've gone.

However, "if you flip around each of those different contentions, you could imagine the sorts of privacy problems that could come up in a different type of app design" where an app is collecting "a lot of data" about a person and "creating a log of where people are going and what they're doing," Butler added.

Since the Biden administration has declined to mandate such vaccine credentials or create a uniform system for verifying statuses, state governments and the private sector will be spearheading these initiatives, which is likely to lead to a variety of approaches based on how local leaders view the privacy, societal and ethical concerns raised by asking for or even requiring proof of a vaccination to participate in commercial activities.

Florida and Texas have moved to ban requiring proof of vaccination to take part in everyday activities such as attending a sporting event or going to a restaurant or movie theater, with Florida Gov. Ron DeSantis arguing that such a move "would create two classes of citizens based on vaccination" and threaten individual freedoms, health privacy and the free flow of commerce.

Similar concerns are likely to be taken into account in other jurisdictions, given that, aside from privacy and data security issues, "use of vaccine credentials raises concerns that unvaccinated individuals could be treated unfairly by employers, businesses, governmental entities or the community at large," said Nicholas Diamond, a director for C&M International, the global policy and regulatory affairs affiliate of Crowell & Moring.

"We must, therefore, ensure that use of vaccine credentials closely hews to core civil rights protections, as well as context-specific protections, such as in the employment setting," Diamond said.

However, while some states are balking at the concept, vaccine credentials are likely to be popular among companies in the U.S. and abroad that are eager to hasten reopening efforts. Therefore, it will be important to monitor how regulators and even the federal government — which has signaled it may at least play some role by offering guidelines on potential standardized proof-of-vaccine credentials — responds to these emerging efforts, attorneys say.

"Since this is still so new, the regulatory response is still unfolding," Zhu said. "When it comes to the collection of personally identifiable information, there are existing statutorily defined penalties and consequences, but the ethical issues it raises are novel, so we're all waiting to see what's going to happen."

--Editing by Aaron Pelc and Emily Kokoll.