Privacy & Data Security Law

Vaccine Passport Success Rests on True Privacy, Equity, Security

By Jodi Daniel, Nicholas Diamond, and Roma Sharma

May 26, 2021, 4:01 AM

Federal leadership on Covid-19 vaccine credentials, through guidance, would minimize risks and advance their development, say Crowell & Moring LLP attorneys and a director with C&M International. That guidance must address accuracy, privacy, and security, and ethical uses of credentials, or we risk unintended consequences that will slow down a safe return to “normal,” they say.

As of May 25, over 164 million Americans had received at least one dose of the Covid-19 vaccine, and over 131 million are fully vaccinated. With an increased focus on re-opening the economy, governments and industry are moving quickly to develop and use Covid-19 vaccine credentials—sometimes called “vaccine passports.” But the risks of moving too quickly are significant.

The Biden administration has said the federal government will neither issue vaccine credentials nor implement a requirement for proof of vaccination. It also will not create a federal vaccination database. However, given the varied state and private sector responses to Covid-19 policies and practices, federal leadership on vaccine credentials, through guidance, would minimize risks and advance the development of Covid-19 vaccine credentials to drive the successful re-opening of the economy.

That guidance must address accuracy, privacy, and security, and ethical uses of credentials. Otherwise, we risk unintended consequences that will slow down a safe return to “normal.”

Ensuring Accuracy and Security

The underlying data and the vaccine credentials themselves must be accurate, reliable, and secure. Since equitable access to vaccine credentials necessitates both electronic and paper options, guidance is required for both. Paper carries the risk of duplication, forgery, and theft. Electronic versions carry similar risks, plus the risk of large-scale data breaches.

Vaccine credential developers should use best practices to authenticate users and devices, and encrypt all electronic data. Paper versions should include scannable codes like QR codes that connect to a secure electronic database.

On the front-end, verification of the site and provider administering the vaccine and providing the information for the vaccine credential is critical to minimize fraud risks. Also, patient identification and vaccination status should be verified by the issuer of the vaccine credential, including verifying timeliness of any required second dose.

On the back-end, corresponding identity verification protocols should be used. For example, any business or university that relies on vaccine credentials should not only review and scan the credential, but also verify the identity of the credential holder using valid government-issued identification, such as a driver's license.

Collecting and Safeguarding Health Data

Data collected for the creation of Covid-19 vaccine credentials should follow well-established privacy principles, such as the fair information practice principles. Health data and other personally identifiable information (PII) collected by companies offering vaccine credentials likely will not be subject to HIPAA protections and other federal or state privacy and security laws are limited. Therefore, building public trust in the privacy of the data will be critical.

Developers and issuers of vaccine credentials should only collect essential data elements. Collection of other PII, such as medical history or geolocation data, could raise privacy concerns. Collecting more data than is needed for a specific, valid, identified use at the time of collection should raise red flags.

Moreover, companies offering vaccine credentials should be transparent regarding data collection and use when individuals register for the credential through simple and easily understood privacy statements, available in several languages.

Strong consideration should be given to limiting the use of PII to the purpose for which it is collected, unless authorized by the individual. Policies for use of de-identified or aggregated data may be more permissive with appropriate protections.

Prioritizing Equity and Ethics

Use of vaccine credentials raises concerns that unvaccinated individuals could be treated unfairly by employers, businesses, governmental entities, or the community at-large. This requires a careful balancing of public health goals and individual liberties.

Some populations may be disproportionally impacted by the use of vaccine credentials. For example, underserved and minority communities disproportionately experience access barriers to vaccinations, including Covid-19 vaccinations. Individuals in rural areas may have difficulty in accessing vaccinations or getting multiple vaccines. Furthermore, many individuals cannot receive the Covid-19 vaccine for health reasons.

Vaccine credentials used as a gateway to re-open the economy risk disadvantaging and potentially discriminating against these groups. Without guidance on recommended uses that accounts for core civil rights protections, as well as context-specific protections like in the employment setting, we miss a critical opportunity to ensure fairness and equity.

Lastly, recommended use of vaccine credentials must follow the science. As we evolve our understanding of the impact of Covid-19 variants and the duration of time over which the vaccination is effective, among other key issues, so too must our approach to recommended uses.

Looking Ahead

The administration can and should provide leadership, while enabling the private sector to develop effective technologies. It might publish guidelines, identify best practices, and align incentives that can be used by technology developers and those implementing and using Covid-19 vaccine credentials.

It also could develop a voluntary certification process to provide for baseline standards and criteria that any vaccine credentialing technology company can attest to meeting. If this is done, a public website could list all vaccine credentialing technologies that meet baseline criteria. This would provide transparency to consumers and allow for accountability based on these public representations.

Regardless of the option, one thing is clear—addressing key issues up front is critical for Covid-19 vaccine credentials to be adopted, and failing to do so risks setbacks to the recovery process that could persist well beyond the pandemic.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Write for Us: Author Guidelines

Author Information

Jodi Daniel is a partner with Crowell & Moring LLP and leads the firm's Digital Health practice. She is also a director at C&M International. She was the founding director of the Office of Policy in the Office of the National Coordinator for Health Information Technology in the Department of Health and Human Services and served as senior counsel for Health IT in the Office of the General Counsel at HHS.

Nicholas Diamond is a director and leads the Global Health group for C&M International, the global policy and regulatory affairs affiliate of Crowell & Moring LLP. He is also an adjunct professor of law at the Georgetown University Law Center.

Roma Sharma is counsel in Crowell & Moring LLP's Healthcare group. She practices regulatory, transactional, and investigational health-care law with a focus on digital health, fraud and abuse, and value-based care.

Law Firms

Crowell & Moring

Topics

forgery
encryption
vaccines
coronavirus
data breaches
health care fraud and abuse