AMA AMERICAN MEDICAL ASSOCIATION

James L. Madara, MD
CEO, EXECUTIVE VICE PRESIDENT

james.madara@ama-assn.org

April 14, 2021

Micky Tripathi, PhD
National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C Street, SW
Washington, DC 20201

Dear Dr. Tripathi:

On behalf of the physician and medical student members of the American Medical Association (AMA), I would like to thank you for collaborative efforts to inform and guide the development of digital vaccine credential services (DVCS). We agree that mechanisms for reliable and accurate certification are important and appreciate your proactive efforts to message the federal government's priorities to relevant stakeholders. As more vaccines are made available and millions of people are vaccinated every day, we are encouraged that the nation may soon round the corner and chart a path away from this pandemic.

However, vaccines are not yet universally accessible, particularly to individuals in historically marginalized and minoritized communities. The use of DVCS should not outpace vaccine availability. Until the time that all Americans are easily able to access vaccines and trusted DVCS, we must guard against programs that appear to confer special social privilege based on one's COVID-19 vaccination status. For DVCS to be successful, vaccines must be universally accessible and the federal government must create strong guardrails around DVCS' use of personal data.

We stress the importance of the federal government's involvement in establishing, publicizing, and enforcing guidelines to which all DVCS must adhere. These guidelines should be developed by federal agencies with experience in consumer data privacy and outline best practices for mitigating inequities and unintended consequences resulting from the development or use of DVCS. We are aware that certain data use practices have been incorporated into codes of conduct (e.g., CARIN Code of Conduct).[1] While such codes are an important first step in establishing guardrails, they are currently unenforceable, have no set process to inform consumers of policy changes, and lack important aspects related to both DVCS specifically and equity generally. Accordingly, DVCS stating they meet a particular code of conduct will not be sufficient. We must remember that inequitable data governance disproportionately harms marginalized communities. This harm occurs even as such communities "are most in need of privacy in order to avoid downstream discrimination and other negative consequences that often results when their sensitive information, including but not exclusively information directly [related] to their minority status, is disclosed."[2] Any credentialing approach must not require the broad or unexpected use of personal information. We expand on these concepts below and have identified several important actions the administration can take to strengthen trust and promote equity by design—both in technology and policy.

[1] https://www.carinalliance.com/wp-content/uploads/2019/05/2019_CARIN_Code_of_Conduct_05082019.pdf.
[2] Skinner-Thompson, Scott (2020-11-04T22:58:59). Privacy at the Margins. Cambridge University Press. Kindle Edition.

Data Minimization and Transparency

Lack of coordination, distrust in technology companies, and inadequate communication led to sluggish adoption of digital contact-tracing applications (apps) last year. Concerns regarding privacy and surveillance dominated the digital contract tracing discussion, leaving little room to explore potential benefits. Often citied were concerns with the amount of information collected by apps and uncertainty, skepticism, and fear around what was being done with data, including with whom it was shared. Seemingly, the assumption was that big tech companies (i.e., Google and Apple) could entice their customers to participate in digital contract tracing by tightly integrating the technology into their products. Yet, it was the lack of tech company oversight and trust that led individuals to doubt the utility and safety of digital contact tracing tools—and which ultimately contributed to their low rate of adoption. Vaccine credentialing apps are likely to face similar concerns regarding privacy, surveillance, and apprehension.

A DVCS—that is, a digital vaccine credential issuer, a digital vaccine credential app/platform, or a digital vaccine credential requestor—should limit the data collected on the individual. Surveys continue to show that individuals distrust business' use of their personal data—particularly when it falls outside the protections of the Health Insurance Portability and Accountability Act (HIPAA).[3] Decades-old federal privacy principles such as data minimization, the "right to be forgotten," and clear data retention polices should be required practices for DVCS.[4] Entities should be prohibited from requiring individuals to create customer accounts to use vaccine credentialing, each of which can impede access for individuals with disabilities, limited English proficiency, or minimal digital literacy. Moreover, DVCS should provide opt-in options for data collection, use, and disclosure rather than registering individuals automatically (i.e., opt-out). As a core technical design tenet, the app and its back end should only collect and store data necessary for the app to function as a credential. DVCS should not make use contingent on individuals' registration for unrelated commercial services or the collection of personal data for unrelated purposes. Failure to include these commonsense approaches will perpetuate the deprivation of privacy rights among historically marginalized and minoritized communities with no meaningful opportunity to avoid data collection—leading to associated marketing at best and targeted harassment of certain communities at worst.[5] This essentially creates classes of individuals whose data is obtained, manipulated, sold, and used to create profiles based on choices not entirely their own. For example, individuals reliant on certain modes of public transportation may be de facto "required" to both obtain a vaccination and use DVCS just to commute to work.

---

[3] https://www.pewtrusts.org/en/research-and-analysis/articles/2020/09/16/americans-want-federal-government-to-make-sharing-electronic-health-data-easier.

[4] *See* Federal Trade Commission's Fair Information Practice Principles, available at https://web.archive.org/web/20090331134113/http:/www.ftc.gov/reports/privacy3/fairinfo.shtm via the Wayback Machine (March 31, 2009).

[5] The COVID-19 Policy Playbook II, published by Public Health Law Watch, describes historical discrimination against communities based on a perceived association with a communicable disease: "Communicable disease epidemics generally trigger widespread fear and the spread of insidious misinformation that unfairly blames marginalized groups for spread of the contagion. As early as the mid-1300s, white Europeans blamed Jewish people for transmission of the bubonic plague throughout the continent (McNeil, Jr., 2009). Americans scapegoated Haitian immigrants and sexual minorities as responsible for HIV transmission in the 1980s (Cohen, 2007). The same fate attended to Mexican Americans during the 2009 swine flu outbreak, West Africans during the 2014 Ebola epidemic, and, of course, Chinese Americans during the COVID-19 pandemic (Lee, 2020). These attacks on marginalized groups during public health emergencies incentivizes them to avoid data collection due to fear of law enforcement dragnets and other punitive measures. Burris, S., de Guia, S., Gable, L., Levin, D.E., Parmet, W.E., Terry, N.P. (Eds.) (2021). COVID-19 Policy Playbook: Legal Recommendations for a Safer, More Equitable Future. Boston: Public Health Law Watch. Available at https://www.publichealthlawwatch.org/covid-playbook-ii.

By promoting strong, clear, and enforceable guardrails around data minimization and transparency, the Biden Administration can send a powerful message about the potential benefits of DVCS, while conferring moral dignity and respect to individuals that also serves to make them "more fit for social participation and contribution, thus benefiting group life."[6]

Application Registration

Built-up demand for social events, indoor activities, and travel may spur significant interest from both businesses and individuals to show proof of COVID-19 vaccination or testing. Yet, DVCS policy is likely to shift as vaccine availability increases and scientific evidence of effectiveness or limitations grows.[7] DVCS will need updates to accommodate these changing requirements. We are also aware that nearly 20 DVCS are being developed at this time, and coalitions are developing technology frameworks for third-party adoption—potentially expanding the number of credentialing apps. No one organization, app marketplace, or industry will be able to track, monitor, and provide individuals meaningful information on credentialing services, including data use policies or app adherence to development principles. Individuals should have access to a single source of truth where they can clearly understand features, functions, and the policies by which apps abide.

Given the role digital vaccine credentials could play as we return to our daily lives, we must also consider what can be done to prevent the creation or exacerbation of inequities. Particular attention should be paid to ensuring DVCS are designed to meet the needs and concerns of historically marginalized and minoritized individuals and communities, including, but not limited to those subject to disproportionate rates of incarceration and heightened surveillance based on immigration status or race; those with stigmatized health conditions such as substance use disorder, HIV/AIDS, and other sexually transmitted infections, LGBTQ individuals, unhoused people, and individuals with disabilities may be wary of DVCS due to the possibility that third parties will share their data with employers, insurers, landlords, the police, or other government agencies.

Federal registration of DVCS would help boost trust. This should be managed by an agency whose stated purpose is the protection of consumers from unfair and deceptive practices—with broad jurisdiction across the economy. Public trust in institutions, both private and governmental, develops slowly and has suffered in recent years. To bolster trust, the federal government should establish a public-facing, centralized website listing DVCS registered with the federal government. **One or more federal stakeholders with experience in consumer protection should create and publicize a set of guidelines to which all DVCS must adhere.** At a minimum, such guidelines should outline best practices for mitigating disparities and implementing equitable data governance principles such as data minimization. Additionally, the pandemic has demonstrated our country's stark disparities in access to technology access, inequitable technology innovation and design priorities, and digital literacy. Any potential DVCS must ensure that individuals can access their credentials in hard copy. **We recommend the administration include in its guidance a requirement that DVCS functionality, content, user interface, and service access of such advanced technologies are designed in an equity-centric participatory fashion with and for historically minoritized and marginalized communities, including addressing culture, language, digital literacy ability, and broadband access.**

---

[6] Bridges, Khiara M. (2017-06-26T23:58:59). The Poverty of Privacy Rights. Stanford University Press. Kindle Edition.

[7] https://www.nejm.org/doi/full/10.1056/NEJMp2104289.

We also recommend that the U.S. Digital Service work with federal agencies to create (1) a system by which DVCS can register with the federal government after meeting certain standards, and (2) a public-facing list of all registered DVCS, with clear and understandable information available about each DVCS—similar to the Centers for Medicare & Medicaid's Blue Button 2.0 initiative.[8] As with Blue Button 2.0, the listing would not be an endorsement of any app, but rather a collection of descriptions of apps that meet certain requirements.[9] While we recognize this would not be easy to do in a short amount of time, we believe it would provide the public with critical insight into what DVCS are trustworthy and align with their privacy values. Furthermore, the federal government should establish a simple process for individuals to file complaints about bad actors and commit to strict enforcement of available laws and regulations. Without oversight or credible information about app developers, individuals may be rightly hesitant to share their health information with DVCS.

Focused Scope of Credentialing Services

Consumer applications by their very nature can provide a highly customized experience for the end user. We have grown accustomed to using applications that perform unique and specific roles such as requesting a ride-share service, order food delivery, or check the weather. However, while we can use one app to order a ride, track its progress, and pay at our destination, several supporting third-party applications, services, and data feeds function together in an orchestration to provide us that experience. App developers are not always forthright or knowledgeable about how information is collected or used by these third parties. By downloading and using these apps, individuals are exposing personal information to dozens of third-party technology companies, ad networks, data brokers and aggregators. News articles have shown that dating, pregnancy, and religious apps send personally identifiable information to groups like Facebook, Google, and Amazon.[10] What may have seemed to be an app built for a specific purpose turned out to be a conduit for tech companies to siphon personal information from unwitting individuals.

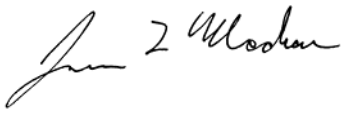
DVCS may start off narrowly focused on providing digital COVID-19 vaccine credentialing services or COVID-19 testing verification. However, without clear federal guidance, app developers may significantly broaden their use case. Adding new functions could invite third-party access to sensitive medical information. Expanding health history for research, sharing non-immunization information with health agencies, or creating personal health records is outside the scope of what a reasonable individual would expect from a vaccine credentialing app. Unanticipated use of data collected for pandemic response may sow additional mistrust in vaccination efforts. An individual may be unaware that once they download an app, automatic updates and patches happen behind the scenes. These kinds of updates could expand the scope of data collected by the app without the individual's knowledge. People should be able to trust that vaccine credentialing apps will be used as intended; they should not be expected to opt-out of unnecessary features or functions. **Accordingly, federal guidelines should include clear guidelines around personal health information (PHI) and personally identifiable information (PII) use, as well as data collection sun-setting provisions on DVCS.**

We reiterate our support and appreciation for the Administration's efforts to guide the development of reliable and accurate DVCS. Incorporating the recommendations in this letter will strengthen the overall effectiveness of DVCS and ensure DVCS are designed with equity in mind while also bolstering public

[8] https://www.medicare.gov/manage-your-health/medicares-blue-button-blue-button-20/blue-button-apps.
[9] https://www.medicare.gov/manage-your-health/medicares-blue-button-blue-button-20/find-apps-to-use-with-medicares-blue-button.
[10] https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html

trust in appropriate access and use of their personal information. Should you have any questions, please contact Matt Reid, Senior Health IT Consultant, Federal Affairs, at matt.reid@ama-assn.org.

Sincerely,



James L. Madara, MD