AMA
AMERICAN MEDICAL ASSOCIATION

James L. Madara, MD
CEO, EXECUTIVE VICE PRESIDENT

james.madara@ama-assn.org

September 22, 2021

Mr. Bill McBride
Executive Director
National Governors Association
Hall of States
444 North Capitol Street NW, Suite 267
Washington, DC 20001

Dear Mr. McBride:

On behalf of the American Medical Association (AMA) and our physician and medical student members, I write to thank the National Governors Association (NGA) for its continued, proactive, and thoughtful response to the COVID-19 pandemic and its commitment to making COVID-19 vaccines available to everyone across the nation. The NGA and state governors have demonstrated leadership in addressing the pandemic from the beginning and managing the ongoing economic and public health threat and uncertainties posed by COVID-19. The AMA also greatly appreciates the NGA's receptiveness to recommendations that the AMA has provided to Governors in prior correspondence.

Today, I write to the NGA and its member governors, to express our concerns about digital vaccine credential services (DVCS). DVCS collect information about a person's vaccination status and use that information to digitally confirm, e.g., via smart phone application (app), whether or not a person has been vaccinated. It is certainly important to have mechanisms in place that reliably and accurately certify that individuals have been vaccinated for COVID-19. Not everyone in the U.S. and within each state across the nation, however, has the same access to the technology whereby their vaccination status may be registered and confirmed. This is particularly true with respect to individuals in historically marginalized and minoritized communities. Also, data about a person's vaccination status constitute personal health information, and safeguards must be taken to ensure that this information is not used for purposes other than vaccine confirmation, such as sale to third parties. The collection of information concerning whether or not a person has been vaccinated must also **not** be used as an opportunity by DVCS to collect and exploit more information than necessary for vaccine confirmation, e.g., driver's license information, date of birth, other health conditions, etc.

Given these concerns, we urge state governors to ensure the following: (1) that DVCS are provided to all state residents on an equal and voluntary basis; (2) that DVCS transparently provide privacy and security safeguards to protect the confidentiality and integrity of the vaccination information in their possession; and (3) that DVCS collect no more information than is necessary to confirm vaccination status. Guidelines applicable to DVCS should be developed by state agencies with experience in consumer data privacy and civil rights and should outline best practices for mitigating inequities and unintended consequences resulting from the development or use of DVCS.

Codes of conduct by themselves are not enough

We are aware that certain data use practices have been incorporated into codes of conduct (e.g., CARIN Code of Conduct),[1] and some DVCS may represent that they comply with an existing data use code or codes of conduct. While such codes are an important first step in establishing guardrails, they are currently unenforceable, have no set processes 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.

Also, it is critical to 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 governors can take to strengthen trust and promote equity by design—both in technology and policy.

Data minimization and transparency

Lack of coordination, distrust in technology companies, and inadequate communication led to sluggish adoption of digital contact-tracing apps last year. Concerns regarding privacy and surveillance dominated the digital contact tracing discussion, leaving little room to explore potential benefits. Often cited 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 (e.g., Google and Apple) could entice their customers to participate in digital contact 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 and state medical records confidentiality laws.[3] Decades-old 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.

As the NGA knows, many states are considering legislation to formally implement these principles on a comprehensive scale, without restricting them to a single, discrete issue such as DVCS. For example, California, Colorado, and Virginia have enacted data minimization and transparency requirements; give

[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.
[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).

their residents the right to have their personal information deleted (among many other rights); prohibit companies from making persons set up a new account in order to exercise their rights; address the length of time personal information may be retained; and specify and limit the purposes for which personal information can be used, etc. Many states considered comprehensive privacy proposals this year, and we anticipate that this trend will only grow stronger. Enacting consumer-protection guidelines of the type described in this letter is entirely consistent with this trend. Moreover, states that implement robust DVCS guardrails around consumer privacy and data governance will take a critically needed step towards fortifying public trust in new and innovative digital tools that stand to improve the nation's health.[5]

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.[6] This essentially creates classes of individuals whose data are 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 use DVCS just to commute to work. By promoting strong, clear, and enforceable guardrails around data minimization and transparency, the NGA and its constituent governors 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."[7]

Application registration

Pent-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 scientific evidence of effectiveness or limitations of vaccines grows.[8] DVCS will need updates to accommodate these changing requirements. We are also aware that nearly 20 DVCS are being

---

[5] As many states learned during the summer of 2020, inconsistent and non-transparent guidance around how digital contact tracing apps collected and shared health and demographic information stymied the adoption and use of such tools, representing a missed opportunity for technology to serve as a supplement to traditional public health surveillance and contact tracing. *See* Timberg, C. et al. "Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for Big Tech's plan to slow the pandemic." *The Washington Post*. April 29, 2020. Available at https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/.

[6] 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.

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

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

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. It is critical to note that these historically marginalized and minoritized individuals and communities 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.

State registration of DVCS would help boost trust and foster consumer protection. This should be managed by an agency whose stated purpose is the protection of consumers from unfair and deceptive practices, such as the state attorney general. Public trust in institutions, both private and governmental, develops slowly and has suffered in recent years. To bolster trust, the states should establish a public-facing, centralized website listing registered DVCS. One or more stakeholders with experience in consumer protection should create and publicize a set of guidelines to which all DVCS endorsed by state governments or used by business entities licensed in the state must adhere. At a minimum, such guidelines should outline best practices for mitigating disparities and implementing equitable data governance principles such as data minimization and transparency. 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 and provide a toll-free number where consumers may have their questions or concerns addressed by designated staff at the DVCS. **We additionally recommend that state guidelines include a requirement that DVCS functionality, content, and user interface are designed in an equity-centric participatory fashion with and for historically minoritized and marginalized communities, including addressing cultural considerations, primary languages other than English, digital literacy ability, and broadband access.**

Consumer protection could also be enhanced greatly if the state made available and publicized a listing of registered apps that satisfied specific requirements issued by the state in its guidelines. This identification would not be an endorsement of any app, but rather a collection of descriptions of apps that met the applicable requirements outlined in the state guidelines.[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 state 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—stalling the important reopening efforts of state governors.

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, ordering food delivery, or checking 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.[9] 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. Without clear guidance, however, 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, the state's DVCS guidelines should include clear guidance around use of personal health information and personally identifiable information, as well as data collection sun-setting provisions.**

We thank you for the opportunity to express our views on this important issue. Please contact Wes Cleveland, JD, Senior Attorney, AMA Advocacy Resource Center at wes.cleveland@ama-assn.org to further discuss the issues raised above. We look forward to determining how our two organizations can work together moving forward on these critical issues.

Sincerely,

James L. Madara, MD

[9] https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html