

April 23, 2021: Advocacy Update spotlight on strong privacy guardrails needed for vaccine credentials

Strong privacy guardrails are needed for vaccine credentials

Digital vaccine credentials systems (DVCS)—also known as “vaccine passports”—may provide an opportunity for people to gain access to social events, indoor dining and travel by providing a mechanism to prove they are vaccinated against COVID-19.

While vaccine credentials are not new, and for years have been necessary for international travel and school-aged children, the desire to digitize credentials raises data privacy and health equity concerns. In a letter to the Office of the National Coordinator for Health Information Technology (ONC) (PDF), the AMA cautions that the U.S. must guard against programs that appear to confer special social privilege based on one’s COVID-19 vaccination status. For DVCS to be successful, the federal government must create strong guardrails around DVCS’ use of personal data. The federal government is providing coordination and guidance rather than direct oversight of DVCS development, implementation and use. Yet, nearly 20 separate DVCS are under development and many are funded by large for-profit technology companies. Traditional federal protections, like the Health Insurance Portability Accountability Act (HIPAA), are unlikely to apply to most DVCS. The AMA’s letter also notes that careful consideration must be given to “what can be done to prevent the creation or exacerbation of inequities” through the use of DVCS.

To bolster the public’s trust in DVCS, the AMA is recommending that the administration establish privacy-preserving and health equity guardrails, including:

- Limiting the data collected on individuals.
- Barring DVCS from requiring people to create customer accounts to use vaccine credentialing.
- Provide opt-in choices for data collection, use and disclosure rather than registering people automatically.
- Only collect and store the data necessary for the app to function as a credential.
- Not be tied to unrelated commercial services or the collection of personal data for unrelated purposes.

The AMA is urging federal agencies to create:

- | A system which DVCS can register with the federal government after meeting certain standards.
- | A public-facing list of all registered DVCS, with clear and understandable information available about each DVCS.

Lacking these commonsense approaches, DVCS could perpetuate the deprivation of privacy rights among historically marginalized and minoritized communities with no meaningful opportunity to avoid data collection—leading to marketing and targeted harassment of certain communities. The AMA will continue to monitor the evolution of DVCS and be engaged with private and public stakeholders.

More articles in this issue

- | April 23, 2021: National Advocacy Update
- | April 23, 2021: State Advocacy Update
- | April 23, 2021: Advocacy Update other news