Outdoorsville's technical and ethical criteria for a digital immunity credential

ELIZABETH NASH, LADAN NASSERIAN, BRIAN SAGER, TONY SEBRO

The goal of this document is to outline the technical and ethical standards for a digital immunity credential for which Outdoorsville should advocate at the federal level. These clear standards reflect a baseline criteria regarding privacy, data protection, and transparency, and will support an inclusive application of an immunity credential (or "passport") for all Outdoorsville citizens and visitors.

In addition to the below, a prerequisite for the following requirements is that the passport should articulate a scientifically-supported minimum benchmark for COVID-19 immunity, to indicate that passport holders are protected from illness.

TECHNICAL REQUIREMENTS

INTEROPERABILITY

- The system should store data in a web-based standard that promotes interoperability.
- The system should comply with other applicable standards and norms for health data, such as the Health Insurance Portability and Accountability Act (HIPAA).
- The system should record the administration of vaccines that have yet to be approved for use in the United States, so that, should the FDA approve their usage at a later date, those preexisting vaccination records can be integrated into the system.
- As best as it can, the system should attempt to be linked to internationally agreed upon specifications and standards.
- Any associated mobile apps on the system should be available on both Android and iOS.
- Vaccine credentials should be accessible online and offline.

METADATA

- The system should maintain metadata about when a user is vaccinated, in case this information becomes useful and actionable as we learn more about COVID-19, vaccine efficacy, and the mutation of new strains.
- The system should accommodate differences between vaccines and their efficacy, as well as efficacy against emerging COVID-19 variants.

SECURITY

- Any personal data collected by the system must be securely stored. The app should encrypt personal data both on the device and in transit.
- The system should follow the principle of least privilege, providing the minimum necessary privilege to perform the job or task.
- Conditions of use of the credential should be clearly presented, understood, and accepted by passport holders.

ETHICAL REQUIREMENTS

OPT-IN ONLY

- Data collection should be opt-in, with users maintaining control over their personal data.
- Businesses and facilities should not be compelled to use the system; they should be able to opt-in as well.

EQUITY OF ACCESS

- The system should not be used to restrict access to essential services.
- The system should only be implemented in jurisdictions where the vaccine is available to every-

one, with no eligibility restrictions.

- The system should be portable, to allow for non-mobile users to provide paper copies or more flexible formats.
- The solution should be affordable for individuals and governments, with resources to develop and sustain the solution.
- The system should have clearly defined uses.
- The system should avoid discrimination and exacerbating existing inequalities such as vaccine hesitancy in certain groups, uncertainties with regard to pregnant women, differential roll-out, or access and digitial divides.

OFFLINE FUNCTIONALITY

- The system should support offline functionality, e.g., the ability to export a printable QR code.

DATA MINIMIZATION

- The system should not track unnecessary data or use third-party tracking or dependencies.
- Any use of personal data should be clear and transparent.
- The system should store personal data for the minimum time period required to maintain system efficacy.

OPEN SOURCE

- The system's code should be open source, both the application and on the server end, in order to promote transparency, engender trust, facilitate broad adoption, and crowdsource the identification and fixing of vulnerabilities.