# Combatting COVID While Protecting Privacy: the Public Health Emergency Privacy Act (PHEPA)

As Americans seek to protect their health during the COVID-19 pandemic and states begin to reopen their economies, new technologies and digital data collection efforts, such as contact tracing apps, have held themselves out as tools to combat the spread of this deadly virus.

While we have come to expect our sensitive health information to be kept private – thanks to the strict rules of the Health Insurance Portability and Accountability Act (HIPAA) – digital contact tracing, symptom tracking apps, and health screening sites are not covered under HIPAA. As a result of this shortcoming, one recent poll found that nearly half of Americans would not use a digital contact tracing app out of concern of misuse of their information. Adding to fears of privacy intrusions, COVID-19 has called attention to stark health disparities among racial, ethnic, and socioeconomic groups. With myriad past examples of algorithmic systems reproducing bias and infringing civil rights, we must ensure that new data collection and processing efforts do not exacerbate inequalities in our society.

Americans will only participate in public health efforts if they trust their information will be safe and secure. Our legal safeguards should catch up to technology. We must ensure governance measures that promise durable privacy protections and protect fundamental rights.

The "Public Health Emergency Privacy Act" would:

- Ensure that data collected for public health is strictly limited for use in public health;
- Explicitly prohibit the use of health data for discriminatory, unrelated, or intrusive purposes, including commercial advertising, e-commerce, or efforts to gate access to employment, finance, insurance, housing, or education opportunities;
- Prevent the potential misuse of health data by government agencies with no role in public health;
- Require meaningful data security and data integrity protections – including data minimization and accuracy – and mandate deletion by tech firms after the public health emergency;
- Protect voting rights by prohibiting conditioning the right to vote based on a medical condition or use of contact tracing apps;
- Require regular reports on the impact of digital collection tools on civil rights;
- Give the public control over their participation in these efforts by mandating meaningful transparency and requiring opt-in consent;
- Provide for robust private and public enforcement, with rulemaking from an expert agency while recognizing the continuing role of states in legislation and enforcement.

The Public Health Emergency Privacy Act ensures that public health authorities and epidemiology researchers can meaningfully access emergency health data, while establishing strict oversight over broader uses of this data. The Act avoids adding further burden on healthcare providers and public health agencies that are covered under HIPAA or other strong, existing privacy regulations.

The Public Health Emergency Privacy Act is endorsed by: Lawyers' Committee for Civil Rights Under Law, Public Knowledge, New America's Open Technology Institute, Consumer Reports, Free Press, Electronic Privacy and Information Center (EPIC), Public Citizen, The AI Now Institute at New York University, Consumer Federation of America, health privacy scholar Frank Pasquale, and privacy scholar Ryan Calo.