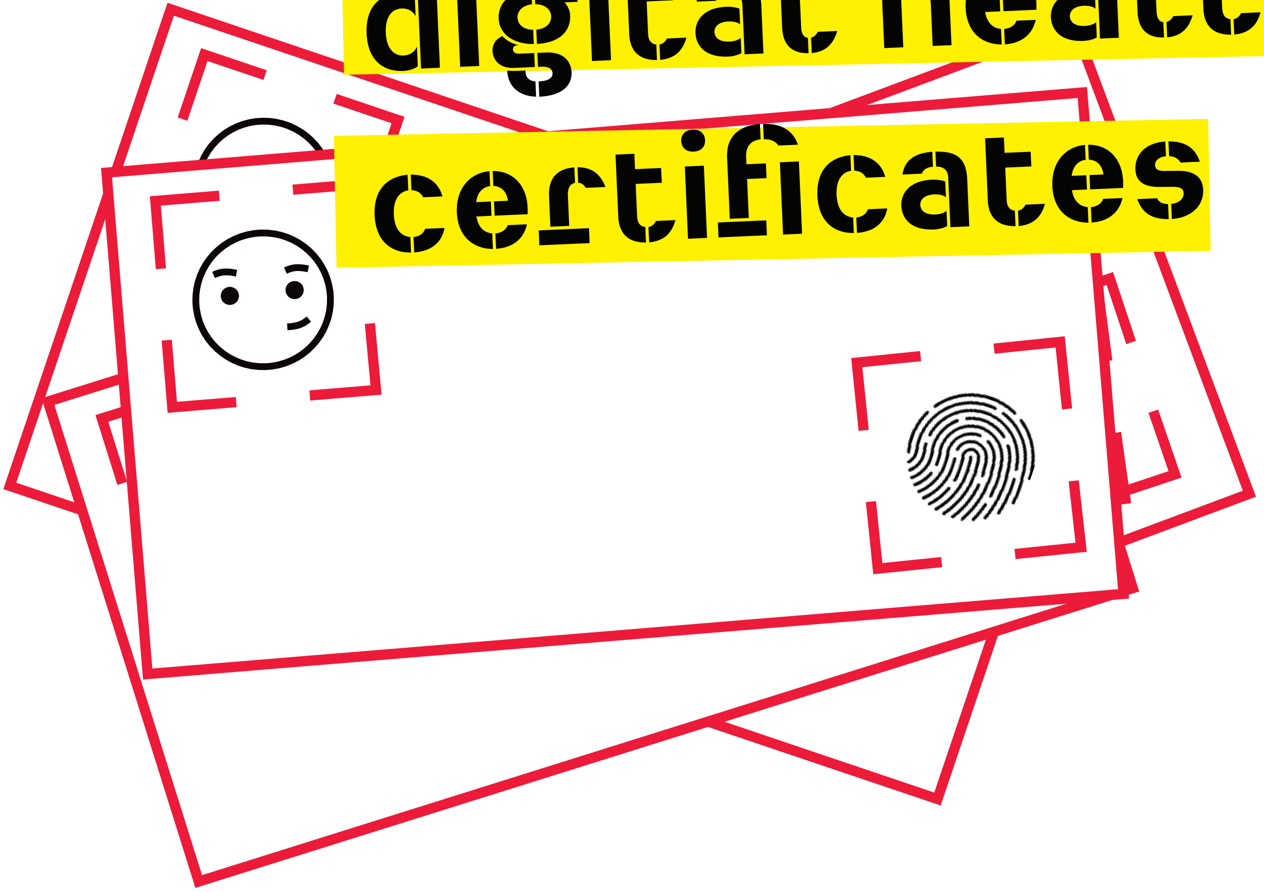
The impact of COVID-19 digital health certificates



accessnow

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

This paper is an Access Now publication. It is written by Naman M. Aggarwal and Carolyn Tackett. We would like to thank the Access Now team members who provided support, including Fanny Hidvégi, Estelle Massé, Verónica Arroyo, Marwa Fatafta, Raman Jit Singh Chima, Carolina Gonçalves, Eric Null, Elizabeth Metts, Juliana Castro, and Sage Cheng. We would also like to thank the #WhyID community for participating in discussions and providing key insights for this publication. We look forward to receiving feedback and further inputs from experts in digital rights, identity, and health.

TABLE OF CONTENTS

JULY 2020

I. INTRODUCTION

Since late 2019, the world has been fighting the novel coronavirus (COVID-19). Governments, nonprofits, companies, and citizens around the world are all responding to the virus and its spread, often looking to technology for possible solutions. At Access Now, we have been keeping track of these developments and their impact on human rights, especially for marginalized communities. We have released specific recommendations on privacy and data protection for technologies being deployed in response to COVID-19, along with specific recommendations for contract-tracing applications.[1] Developing sustainable and effective solutions to combat the virus and its spread requires putting human rights—including the fundamental right to privacy—at the center of both design and implementation.

In this report, we outline the various models of digital health certificates currently under consideration and the human rights concerns such certificates raise. We highlight the importance of a rights-oriented approach in the development of any digital health certificate program.

[1] Access Now, Recommendations on privacy and data protection in the fight against COVID-19, https://www.accessnow.org/covid19-data-protection/; Access Now, Privacy and public health: the dos and don’ts for COVID-19 contact tracing apps, https://www.accessnow.org/privacy-and-public-health-the-dos-and-donts-for-covid-19-contact-tracing-apps/

II. DEFINITION OF DIGITAL HEALTH CERTIFICATES

As some countries and regions transition to the latter stages of responding to COVID-19, governments are exploring how to open up the movement of people—ranging from intra-city to inter-country and cross-border. There have been increasing proposals to use certificates or passes based on individuals' health status to determine who can return to work or enter recreational spaces, emergency response, and more. We refer to such initiatives, in which certification based one's health status is administered and authenticated digitally to allow or disallow movement or access to services, as digital health certificates. While there is precedent for requiring vaccine certificates for travel to specific countries—for example, the yellow fever vaccination required when traveling between countries with differing levels of exposure—the current proposals are on a different scale and are distinguishable from preexisting practices. In contrast to yellow fever, COVID-19 has been confirmed in many more countries, certifying COVID-19 as a pandemic rather than a disease endemic to certain countries.[2] Further, as we note below, the science behind the immunity and antibodies is underdeveloped and thus certainty of protection from COVID-19 is not available.

[2] Elizabeth M. Renieris, Dr. Sherri Bucher, and Christian Smith, "The Dangers of Blockchain-Enabled "Immunity Passports" for COVID-19," Medium, May 18, 2020, https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290

III. BASIS OF CERTIFICATION

Current digital health certificate proposals generally rely on one of two indicators: verification of a person's immunity to COVID-19, which is not yet possible with any scientific certainty, or a determination of someone's risk level based on non-specific environmental factors, which often also rely on unproven technologies.

1. IMMUNITY

Also known as immunity certificates or immunity passports, these programs are intended to certify an individual has gained immunity from a particular disease and thus should be allowed to access designated spaces or services. These certificates are generally issued based on testing that verifies a person has acquired the necessary antibodies or on the administration of a safe and effective vaccine.

While work is ongoing in the development and testing of COVID-19 vaccinations, there is currently no vaccine available. Additionally, research continues on the efficacy of acquired antibodies from the survival of a patient from COVID-19. As per the latest guidance provided by the World Health Organization (WHO) in April 2020, there is no evidence available that a person who survived COVID-19 once is immune from a second infection.[3] It is also unknown how long antibodies may be present in a person's blood, though there is early evidence that antibodies die off quickly in the body.[4] Without such evidence or vaccination, there is no sound case for immunity-based digital health certificates in relation to COVID-19. As the WHO notes, issuance and usage of such certificates may even increase the risks of continued transmission.[5]

2. RISK PROFILE

Because evidence-based certification mechanisms are not currently possible, governments and other stakeholders are exploring alternative methodologies for issuing digital health

[3] "'Immunity passports' in the context of COVID-19," World Health Organization, April 24, 2020, https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19

[4] Charlotte Joe, "Immunity to covid-19 could disappear in months, a new study suggests," MIT Technology Review, July 13, 2020, https://www.technologyreview.com/2020/07/13/1005103/immunity-to-covid-19-could-disappear-in-months-a-new-study-suggests/

[5] WHO, "Immunity passports" in the context of COVID-19, https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19

certificates based on a person's overall level of risk. These methods would construct a "health risk profile" based on various signals such as where a person lives (e.g., zoning specifications in India), existing illnesses that exacerbate risk, and contact tracing (medical and app-based).[6] The risk level associated with a person's profile would then be used to determine where they can travel and what services they can access.

Currently, these systems are largely based on unproven technology and only provide assertions about an individual's health status based on probability and are thus prone to error. Further, these technologies rely on mass collection of sensitive personal data and algorithms for profiling that are largely untested and lack transparency. There is no evidence-based method available to ascertain the risk profile of an individual in relation to COVID-19.

Case Study: India	Aarogya Setu, India's "one-stop solution for everything related to COVID-19," provides an interface for a self-assessment of COVID-19 risks. The assessment asks users to provide some information about themselves, including habits as well as current symptoms. Based on this test, users are marked "safe" or "unsafe." The decision-making protocol for this test is unknown, with high uncertainty around how closely its results correlate to actual exposure risk. The Ministry of Home Affairs in India initially made use of the application's self-assessment tool mandatory for all employees of public and private enterprises.[7] Shortly after, it updated its directive to ask employers to make their "best effort" to enforce use of the app among their employees, but no longer deemed it mandatory.[8] In an analysis of various contact-tracing applications from the *MIT Technology Review*, the Aarogya Setu scored a low 2 out of 5 when it comes to the protection of users and the application's efficacy.[9] The researchers later

[6] "Explained: What are containment zones, how are they demarcated?", Indian Express, https://indianexpress.com/article/explained/coronavirus-cases-india-containment-zones-6487494/

[7] Spokesperson, Ministry of Home Affairs Twitter account, May 1 2020 https://twitter.com/PIBHomeAffairs/status/1256216662900117506

[8] "Aarogya Setu: MHA Dilutes Mandatory Imposition; Says Employers On 'Best Effort Basis' Should Ensure Use of App By Employees With 'Compatible Mobile Phones,'" LiveLaw News Network, May 17, 2020, https://www.livelaw.in/top-stories/aarogya-setu-mha-dilutes-mandatory-imposition-156921

[9] Patrick Howell O'Neill, "India is forcing people to use its covid app, unlike any other democracy," MIT Technology Review, May 7, 2020, https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/

downgraded the rating from 2 to 1 because the app collected far more data than was required.[10]

In a recent development, the privacy standards of the application were again changed. These updates have allowed the application to upload even more of a user's data to the central server, irrespective of the user's COVID status. The update has also allowed users to access information such as the date, time, approximate location, and duration of a "Bluetooth contact" who has been diagnosed with COVID-19.[11]

[10] Aditya Chunduru, "After MIT tech review downgrades Aarogya Setu rating, source code for app made public," Deccan Chronicle, May 27, 2020, https://www.deccanchronicle.com/technology/in-other-news/270520/after-mit-tech-review-downgrades-aarogya-setu-rating-source-code-for.html

[11] Aarogya Setu Twitter account, July 5, 2020, https://twitter.com/SetuAarogya/status/1279634258072465409

IV. IMPACT ON THE RIGHTS OF USERS

While the primary concern regarding digital health certificates currently remains the lack of an effective and evidence-based solution, there are multiple other human rights concerns that need to be addressed.

1. RIGHT TO PRIVACY

Most digital health certificates would require the collection of sensitive personal information, putting individuals' privacy at risk. Health information is private and sensitive by nature and reveals intimate details of a person's life. The use, collection, access, and any other processing of this information should be protected, ideally through a comprehensive data protection law.[12] But most countries considering proposals for digital health certificates have either a weak or outdated data protection framework, or none at all. Further, it is important to note that centralized solutions with centralized storage of information—especially without adequate checks and balances for sharing of data within and between governments—can create mammoth yet fragile identity systems that put both individuals' privacy and data security at risk.

Governments must approach digital health certificates with caution, acknowledging the unique risks of collecting health-related and other sensitive personal data, especially when it may be collected, accessed, or processed by people who are not medical professionals. No one should have to compromise their fundamental right to privacy in order to maintain access to essential services or freedom of movement.

As we have previously noted, in combating COVID-19, public authorities should be able to rely on accurate data, including health data, to determine the best course of action to mitigate the spread of the virus and identify what measures must be taken to safeguard people and their rights both during and after the crisis. However, the use of such data must be grounded in the principles of necessity and proportionality, which may be evaluated through a three-part test. The data collection and use must be:

1. in accordance with or prescribed by law (i.e. the legality principle),
2. necessary to achieve a certain aim (i.e. the necessity principle), and
3. proportionate to the aim pursued (i.e. the proportionality principle).

[12] Access Now, Creating a Data Protection Framework: a Do's and Don'ts Guide for Lawmakers, 2018. https://www.accessnow.org/data-protection-handbook

Jurisdictions around the world have reaffirmed these principles when considering government responses to COVID-19. For example, the Israeli Supreme Court ruled that security forces could not apply surveillance capabilities to tracking COVID-19 patients without legislative approval, and the European Data Protection Supervisor called for any use of location data to be guided by the principles of necessity, proportionality, and effectiveness.[13]

2. RIGHT TO MOVEMENT AND FREEDOM OF ASSEMBLY

Governments and companies are considering using digital health certificates to determine who can travel—both within cities and between countries—as well as who can access public spaces, work spaces, and places of leisure.[14] In most of these use cases, a person would not be allowed to access a particular area unless they possess a digital health certificate. These restrictions may impact people's ability to access essential services, carry out their livelihood, and participate in civic life. It is especially important to have clear safeguards for the freedom of peaceful assembly and association, and to enable essential movements for social, racial, economic, and environmental justice to flourish online and off.

Those in power must not impose digital health certificate schemes that can be leveraged to silence dissent, suppress social movements, or otherwise exert control for purposes other than public health.

3. EXCLUSION

Digital health certificates rely on both the overall presence of digital infrastructure and an individual point of connection such as a mobile phone. These requirements are not realistic for many individuals, especially those in marginalized communities.[15] People without personal mobile phones, communities with inadequate access to digital infrastructure, and

[13] Noa Landau and Netael Bandel, Israel Secretly Sought To Expand Shin Bet Tracking of Coronavirus Patients Before Court Ruling (June 24, 2020), https://www.haaretz.com/israel-news/.premium-israel-secretly-sought-to-expand-tracking-of-coronavirus-patients-before-ruling-1.8801167; https://twitter.com/EU_EDPS/status/1253623503254937600.

[14] See, e.g., Saudi Press Agency, Kingdom's Government Sets Preventive, Precautionary Measures to Prevent COVID-19 Infection Transmission, Interior Ministry Says, https://www.spa.gov.sa/viewstory.php?lang=en&newsid=2043855, (7 March 2020); WorldAware, Saudi Arabia Maintaining Restrictions on Entry of Arrivals, https://www.worldaware.com/saudi-arabia-maintaining-restrictions-entry-arrivals (8 March 2020). In March 2020, the government of Saudi Arabia imposed a restriction on individuals who wish to enter from countries affected by the COVID-19 pandemic, according to a list approved by health authorities. Upon arrival in Saudi Arabia, these people must present a Polymerase Chain Reaction (PCR) certificate proving they are not infected with COVID-19.# The PCR certificate has to be issued within 24 hours of boarding the flight to Saudi Arabia, and the air carrier must ensure that the certificate is valid.

[15] Natalie Kofler and Françoise Baylis, "Ten reasons why immunity passports are a bad idea," Nature, May 21, 2020, https://www.nature.com/articles/d41586-020-01451-0

people with digital literacy problems would face massive exclusion. Further, getting access to a digital health certificate may come with costs. **Access to essential services and movement must not be restricted for any individual due to a lack of access to digital infrastructure.**

4. DISCRIMINATION

COVID-19 has already disproportionately impacted individuals otherwise facing discrimination and marginalization. From the Black community in the United States to indigenous communities in Brazil's Amazon region, we have seen more infections and higher death tolls.[16] Communities who face discrimination often also have reduced access to effective healthcare, fill essential jobs that increase risk of exposure, and are less likely to have access to reliable internet at home, making it more difficult to receive crucial public health information and to observe social distancing. Digital health certificates that restrict freedom of movement create a high risk of reinforcing and deepening these existing inequities in COVID-19's impact. The government of Chile recognized these risks and suspended the rollout of a COVID-19 card.[17] According to Minister of Health Jaime Mañalich, "the fact that a person has a COVID-19 card could give him or her certain privileges compared to another who does not have it, as a priority to be hired or rehired, entering public places and other situations."[18]

Further, there have been multiple instances of stigmatization and resultant discrimination against people with COVID-19 across the world, including online hate speech targeting many vulnerable groups.[19] Beyond legal restrictions, digital health certificates would likely have a heavy social impact, and people without these certificates would have to face undue discrimination by peers, society, their workplace, and the government.[20] In India, for example,

[16] Centers for Disease Control and Prevention, COVID-19 in Racial and Ethnic Minority Groups (June 25, 2020) https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/racial-ethnic-minorities.html; Dom Philips, "'We are facing extermination': Brazil losing a generation of indigenous leaders to Covid-19," The Guardian, June, 21, 2020, https://www.theguardian.com/global-development/2020/jun/21/brazil-losing-generation-indigenous-leaders-covid-19

[17] Minister of Health Twitter account, May 10, 2020, https://twitter.com/ministeriosalud/status/1259512225888448512

[18] "Gobierno posterga por posible "discriminación odiosa" entrega de polémico carnet Covid-19," Diario La Prensa, May 10, 2020, https://new.diariolaprensa.cl/index.php/2020/05/10/gobierno-posterga-por-posible-discriminacion-odiosa-entrega-de-polemico-carnet-covid-19/

[19] Access Now, Fighting misinformation and defending free expression during COVID-19: recommendations for states, https://www.accessnow.org/covid19-fighting-misinformation; Equality Labs, Coronajihad: An Analysis of COVID-19 Hate Speech and Disinformation, https://www.equalitylabs.org/coronajihad/

[20] Carr Center, Examining the Ethics of Immunity Certificates, https://carrcenter.hks.harvard.edu/files/cchr/files/005-covid_discussion_paper.pdf

pharmacy owners have appropriated the contact-tracing app Aarogya Setu for unofficial use, restricting people from entering their stores unless they showed they had installed the app on their phone.[21] Similar response to digital health certificates could result in even greater discrimination, both direct and unintended.

Governments, employers, and others considering these tools must evaluate any mechanism for containing the spread of COVID-19 for its disparate impact on those already facing heightened risk. For digital health certificates—a tool that has not been proven effective by any measure—the risk of harm may significantly outweigh the benefits.

5. CREATION OF PERMANENT HEALTH SURVEILLANCE INFRASTRUCTURE

While digital health certificates are currently being proposed as a temporary and standalone measure for combating COVID-19, there is a real threat that the resultant infrastructure may either be made permanent or integrated into existing digital identity programs or border surveillance systems. We must prevent the crisis from becoming an "opportunity" to establish health surveillance infrastructure across the world.

For instance, the United Kingdom is currently actively considering the use of immunity certificates in the country as a measure to open up movement post lockdown.[22] There are increasing concerns emerging that these initiatives may end up acting as a gateway to a person's ability to access services, employment, and public spaces. Further, these initiatives may be "early explorations" into a Public Health Identity (PHI) system wherein a permanent infrastructure of health identity may be created requiring the sharing of private health information for public health concerns.[23]

In addition to strong frameworks for data protection *during* the COVID-19 crisis, **governments and any other actors collecting or repurposing data as part of a COVID-19 response must adopt clear timelines for erasing health data and other sensitive information — including geolocation data and information about personal contacts and community networks.**

[21] Pranav Dixit, "For A Billion Indians, The Government's Voluntary Contact Tracing App Might Actually Be Mandatory," BuzzFeed News, April 30, 2020, https://www.buzzfeednews.com/article/pranavdixit/for-a-billion-indians-the-governments-voluntary-contact

[22] Chris Smyth and Tom Whipple, "Immunity forms planned for coronavirus survivors," The Times, May 22, 2020, https://www.thetimes.co.uk/article/immunity-forms-planned-for-coronavirus-survivors-6gz0szlhw

[23] Imogen Parker and Elliot Jones, "Something to declare? Surfacing issues with immunity certificates," Ada Lovelace Institute, June 2, 2020, https://www.adalovelaceinstitute.org/something-to-declare-surfacing-issues-with-immunity-certificates/

VI. CONCLUSION

The response to COVID-19 has prompted many solutions and approaches from all quarters. This is an unprecedented crisis and must be met with innovative and bold solutions, centered around the protection of people's health and their rights. But we must guard against the tendency of targeting individuals rather than the virus. Any and all measures against COVID-19 must protect the rights of individuals, for only in such a circumstance would we be able to come up with sustainable solutions to the crisis.

In particular, governments and other actors considering digital health certificates as part of their COVID-19 response should, above all, only move forward with proposals that are based on strong scientific evidence of their effectiveness, built with technologies that are vetted for their security and stability, and designed to mitigate human rights impacts, especially for those who are most vulnerable.

> *"Asking people to choose between privacy and health is, in fact, the very root of the problem. Because this is a false choice. We can and should enjoy both privacy and health. We can choose to protect our health and stop the coronavirus epidemic not by instituting totalitarian surveillance regimes, but rather by empowering citizens."* — Yuval Noah Harari [24]

For more information, please contact:
Naman M. Aggarwal | Global Digital Identity Lead, Access Now | naman@accessnow.org

[24] Yuval Noah Harari, "The world after coronavirus," Financial Times, March 20, 2020, https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75