Review Article

DIGITAL HEALTH

DIGITAL HEALTH
Volume 10: 1–17
© The Author(s) 2024
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20552076241239171
journals.sagepub.com/home/dhj
Sage

Scoping review of data privacy risks in COVID-19 apps with digital vaccination certifications

Isca Amanda, Savannah Graffin and Maria Adela Grando

Abstract

The goal was to review mobile apps with COVID-19 digital vaccination certificates between November 2022 and March 2023 and evaluate: (a) compliance with the WHO Proof of Vaccination Scenario requirements, (b) risk levels of app permissions using a Permission Accumulated Risk Score (PARS), and (c) readability and transparency of the app's privacy policies using a Privacy Transparency Index (PTI) score. We found 49 mobile apps with COVID-19 digital vaccination certificates from across 32 countries. Most apps were developed by governments (37/49, 75.51%). We discovered a high positive correlation between the country-wide app total installs and the people vaccinated with at least one dose in the country ($r = 0.93$, $P = <.001$). Most apps (97.96%) had sources of information available for compliance with WHO Proof of Vaccination Scenario requirements. Only two apps included all the required data items, while most apps (75%) included five or more data out of nine items. We found that most (97.96%) apps had a Google Play link to generate the Exodus platform permission report, and most (95.92%) apps had an associated privacy policy available. We identified 80 unique permissions; some (23.75%) were dangerous or special. We also found 28 types of trackers. The average PARS was 28.58 (IQR 23.25, range 15–38.25). Most of the apps' privacy policies documents were difficult or very difficult to read (median grade level 14, IQR 2.6, range 13–15.6). The average PTI was 50.43 (SD 14.73; range 22.5–75). In conclusion, higher compliance with the WHO Proof of Vaccination Scenario requirements is desirable to support interoperability. Developers should limit the number of permissions for essential needs and disclose their purpose. Developers should write privacy policies that a wider audience can understand.

Keywords

Apps, mobile health, systematic reviews, studies, public health, health informatics

Submission date: 25 May 2023; Acceptance date: 27 February 2024

Introduction

In March 2020, the World Health Organization (WHO) declared the COVID-19 pandemic.[1] To avoid spreading the virus, lockdowns, stay-at-home, work-from-home orders, and travel restrictions were implemented. As of April 2022, 19 vaccines have been authorized for emergency use, and 12 were fully approved vaccines worldwide.[2]

Proof of COVID-19 vaccination was required to keep track of an individual's COVID-19 vaccine record and compliance with travel restrictions. A vaccination certificate is a type of health documentation that tracks and records vaccinations administered to an individual and contains basic demographics about the individual, the name of the administered vaccine, the date of the dose administered, and other data items.[3] Digital vaccination certificates are records in electronic format for all immunizations an individual has received that are accessible to the individual and authorized health workers. A one-dimensional or two-dimensional barcode establishes the link between a paper vaccine record and a digital vaccine record.

According to WHO, Digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS) is defined as "a type of digital documentation that is used to represent the COVID-19 vaccination status of an

College of Health Solutions, Arizona State University, Phoenix, Arizona, USA

Corresponding author:
Maria Adela Grando, College of Health Solutions, Arizona State University, 6161 E Mayo Blvd, Phoenix, Arizona, 85054, USA.
Email: agrando@asu.edu

individual."[3] This digitally signed document is based on healthcare standards—such as the Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) —to uniformly specify data in the document's core data set. A DDCC:VS document can support Continuity of Care and Proof of Vaccination scenarios. For the Proof of Vaccination scenario, a DDCC:VS may be inspected by an interested party during coverage monitoring surveys, after testing positive for COVID-19, for work and education purposes, and for traveling internationally.[4] DDCC: VS also supports barcodes to support links to paper vaccine records.

Data privacy could be at risk with digital vaccination certificates in COVID-19 apps. Some risks of data privacy with personal identifiable information (PII) can include carrying a photograph of the physical vaccine card on a user's device, connecting a device to an unprotected WiFi or Bluetooth signal, using apps with state-maintained databases embedded in the app's system, or using third-party developed apps that could have varied security measures.[4] Lack of appropriate safeguards, lack of encryption, mobile malware, access to the software by a third-party, and outdated security software are some privacy risk examples of technical measure problems that could arise.[5]

The Republic of Indonesia developed the PeduliLindungi app to help tracking and screening COVID-19 statuses.[6] However, in September 2021, their President's vaccine certificate got leaked online, one month after a suspected breach of its sister app, Indonesia Electronic Health Alert Card (eHAC) app. The eHAC breach was enabled by the app developers' failure to implement appropriate data privacy protocols. PII data for over one million citizens got exposed on an open server as well as the app's entire infrastructure that includes hospitals' private records, including those from Indonesian officials that used the app.[7,8]

The root cause of data privacy problems within digital apps can vary. The reduced ability to maintain data security is associated with increases in app data collection, increases in maintenance costs, and challenges associated with maintaining data privacy regulations. For instance, a health app named Docket that focuses on storing digital vaccination certificates experienced a bug that allowed all users to access any other users' PII and vaccine information in late 2021.[9]

There is a need for readable and transparent privacy policies for digital vaccination certificates in COVID-19 apps. Mobile operating systems provide safeguards against unauthorized access to PII, and apps must request permission from users for these services prior to installation or at runtime.[10,11] Privacy policies can make the user aware of the personal data collection and sharing practices that are in place. However, often privacy policies are not effective because they are lengthy and/or use convoluted legal language.[11,12] While having more readable privacy policies and understanding the data privacy risks of an app will not reduce the potential for unauthorized access, it may help the users decide if they want to install the app, choose between alternative apps, or limit the amount of personal information users input into it. This could reduce the amount of personal information that is lost in the event of a security breach. Often app developers fail to inform users about their data collection and sharing practices, and users make decisions without realizing their consequences.[13,14]

As of October 2021, the status quo is that 144 countries have developed and required COVID-19 vaccination certifications.[15] Despite the abundance of apps, little research has been done on systematically assessing their (a) compliance with the WHO DDCC:VS Proof of Vaccination Scenario Requirements, (b) data privacy risk levels, and (c) readability and transparency of their privacy policies. Our research goal was to conduct a scoping review to assess a), b), and c) apps that support COVID-19 vaccination certifications. Our motivation was to recommend best practices to reduce data privacy risks and increase consumer trust in COVID-19 apps with digital vaccination certifications.

Background

Mbunge et al. provided 2021 preliminary lessons from studying 13 digital vaccination certification apps.[16] They concluded that COVID-19 digital vaccination certificates may face challenges; these included (1) lack of information and communication technology (ICT) supporting infrastructure, (2) socio-economic disparities, (3) lack of standardized COVID-19 vaccination certificates, (4) inconsistency and heterogeneous digital solution development standards, (5) security risks and privacy, (6) lack of frameworks and global standards/policies, and (7) ethical concerns. Our study provides a systematic way to dive deeper into the challenge (2) by looking into the readability of the app's data privacy policies, challenge, (3) by checking compliance with the WHO requirements, and challenge, (5) by assessing data privacy risk levels of COVID-19 digital vaccination certification apps.

Bardus et al. (2022) conducted a systematic review of data management and privacy policies of 180 COVID-19 contact-tracing apps.[17] Although there are overlaps between contact-tracing apps and digital vaccination certificate apps, our research focused on the second app group. Bardus et al. introduced the Permission Accumulated Risk Score (PARS) to study data privacy risk levels and the Privacy Transparency Index (PTI) to analyze the readability and transparency of the app's privacy policies. They found that contact-tracing apps had a relatively low number of installs. Privacy-preserving apps scored high in transparency and App Store ratings, suggesting users appreciate this feature. They also discovered that privacy policy documents were difficult to read by an average audience. Our work builds on Bardus et al.'s research by adopting the PARS and PTI methods. As a novelty, our study checks the compliance with WHO recommendations on data requirements for proof of vaccination.

Methods

The review of COVID-19 mobile applications with digital vaccination certificates followed Bardus et al.'s approach, consisting of app search, identification, and selection.[17] The process also included data extraction and analyses. In addition, compliance with WHO recommendations on data requirements for proof of vaccination was checked.

Each included mobile application was reviewed to answer the following research questions: (a) Can the app be used to provide WHO-compliant proof of COVID-19 vaccination? (b) Are there data privacy risks associated with the use of the app? (c) Does the app contain data privacy policies that are readable and transparent?

Search queries and sources

COVID-19 apps that include digital vaccination certificates were retrieved on 4 November 2022. Apps were retrieved from the Google Play and the Apple App Store. Similar search terms were used for both platforms (Table 1).

Inclusion criteria

Eligible apps had to (1) retain the information of the user's COVID-19 vaccination status in any form, (2) be free for use, (3) have an English description, and (4) be available within the Google Play. The exclusion criteria were apps that (1) directly scan COVID-19 certifications (scanner apps) or do not support COVID-19 digital vaccination certifications, (2) have a cost, (3) have no English description, and (4) are unavailable in the Google Play.

Table 1. App search queries.

Application store	Search query
Google play store (android)	*immunization|vaccine|vaccination AND certificate|wallet|pass|record|passport|document site:play.google.com*
Apple app store (ios)	*immunization|vaccine|vaccination AND certificate|wallet|pass|record|passport|document site:apps.apple.com*

App selection

The process of app selection was conducted in multiple stages. SG searched for apps within the Google Play and IA searched for apps with the Apple App Store and collected general app information (app name, developer name, country of development, and app rating). The information was extracted into Microsoft Excel for screening. SG and IA screened the selected apps, cross-evaluated each other's work, and resolved disagreements through consensus.

Data extraction and elaboration

App characteristics. The following information was extracted from the Google Play for each app: ratings, number of downloads, number of reviews, link to the privacy policy provided by the developer, and sponsor information. The same information, except for the number of reviews, was extracted from the Apple App Store for each app. SG extracted the information, and IA cross-evaluated the information. Discrepancies were discussed and resolved. App characteristic information was collected in December 2022. IA extracted Our World in Data's cumulative data of people with at least one dose of COVID-19 vaccine in apps' origin countries per 1 December 2022.[18] Then, IA analyzed the vaccine count and app number of installs' correlation using Pearson's correlation coefficient (r) and *p*-value (*P*) from t-statistics.

Proof of COVID-19 vaccination

Available sites (product sites, product store sites, and government sites) and documentation (privacy policies) that include app information were evaluated for identifying data items in the WHO Proof of Vaccination scenario checklist. Apps with no available sites or documentation were excluded from the evaluation. Discrepancies were resolved by consensus. As shown in Table 2, all data items listed in the checklist were evaluated and identified through a yes (1) or no (0) ranking. Only data items with a "required" status were used to compare apps.

Data privacy. The WHO Proof of Vaccination Scenario does not recommend requirements for security and privacy; therefore, we adopted the Permission Accumulated Risk Score (PARS).[17] Table 3 lists the top 18 most dangerous permissions categorized by PARS. For each dangerous permission, we listed app functionalities that could be supported by the permission and examples of potential data privacy risks.

SG extracted app permissions to access users' data and information using Exodus.[19] All permission items were entered into Microsoft Excel. Each permission was classified according to two risk levels: Normal or Dangerous.

Table 2. Checklist and rubric for app sites and documentation used to calculate WHO compliance for proof of vaccination.

WHO item
Required
Name
Date of birth
Vaccine or prophylaxis
Vaccine brand
Vaccine manufacturer or vaccine market authorization holder
Vaccine batch number
Date of vaccination
Dose number
Country of vaccination
Optional
Unique identifier
Vaccination valid form
Total doses
Administrating center
Health worker identifier
Disease or agent targeted
Conditional
Signature of health worker
Not needed
Sex
Due date of next dose

Dangerous data privacy risks allow the app additional access to potentially sensitive data (e.g. location and contact information). The PARS was computed by multiplying the sum of normal risk = 1, dangerous risk = 2, and trackers = 3. The higher the PARS score, the higher the danger to user privacy.

Privacy policies. If privacy policies were unavailable in English from the developer website, they were translated into English using Google Translate.[20] An assessment of privacy policies was conducted by IA and SG using a standardized web-based checklist adopted from Bardus et al. (Table 4). Table 4 contains 13 questions organized in three areas of interest: privacy, data management and legal framework.

Each item from the checklist was ranked (yes = 1, no = 0, or not applicable). Once all items were added, a PTI score was computed. The higher the PTI score, the higher the transparency of the app's privacy policy.

We conducted readability analyses of app privacy policies evaluating the Flesh–Kincaid Grade Level in Microsoft Word.[21] Each available privacy policy was converted into individual Word documents. The lower the readability level of a privacy policy is, the easier it is to be understandable. A paired two-tailed distribution T-test was then calculated the compute the means from IA and SG's individual PTI evaluations.

Data analyses. Descriptive statistics and data analyses were conducted to calculate WHO compliance, PARS, and PTI. WHO compliance was scaled to 100 for cumulative score calculation. A cumulative score was calculated as: WHO compliance + PTI − PARS (range: 100 to 200).

Results

Search results

Figure 1 illustrates the app selection process. We applied the search queries to Google on 4 November 2022. We identified 78 records from the Google Play and 131 from the Apple App Store. After removing duplicate links, we shortlisted unique app links from Google Play (61/78, 78.2%) and Apple App Store (49/131, 37.4%). In the screening stage, we excluded apps from Google Play and Apple App Store that were considered not DDCC:VS apps (22/61, 36.01% and 11/49, 22.45%). Most irrelevant apps were designed to scan or verify DDCC:VS apps. We assessed the remaining for eligibility (39/61, 63.93% and 38/49, 77.55%). Finally, we excluded two apps exclusive to Apple App Store and unavailable in Google Play. The Exodus data privacy risk report[19] only accepts Google Play links and does not support Apple App Store links. *CommonPass* was discontinued and removed from Google Play; we withdrew it from the app selection and data analyses and replaced it with its sister app, *CommonHealth*, on 3 March 2023.

The final app list included 49 unique DDCC:VS apps potentially eligible for review. Of these, most (48/49, 97.96%) apps had sources of information available for compliance assessment to the WHO DDCC:VS Proof of Vaccination Scenario Requirements. Most apps had a Google Play link to generate the Exodus platform risk report (48/49, 97.96%) and had associated privacy policies

Table 3. As categorized by PARS, top 18 most dangerous permissions are listed, with app functionalities that could be supported by the permission, and examples of potential data privacy risks.

Permission	App functionality	Data privacy risk
Access camera	Upload an image of a paper vaccination certification	Unauthorized access to user’s camera and photos
Access fine location	Detect user’s precise location	Unauthorized tracking of user’s precise location
Access coarse location	Detect user’s approximate location	Unauthorized tracking of user’s approximate location
Write external storage	Modify or delete vaccine certification information in app where the contents are stored	Unauthorized access to delete, insert, or update user’s shared storage
Read external storage	Read stored vaccine certification information	Unauthorized access to user’s shared storage
Write settings	Modify or delete phone’s settings	Unauthorized access to user’s phone settings
Access background location	Track user’s location while the app is running in the background	Unauthorized access to user’s location
Call phone	Verbally communicate with paramedics, specialists, and other related physicians over device	Unauthorized calls from the phone
Record audio	Enable audio conference with paramedics and physicians for apps with calling and chatting features	Unauthorized access to device’s audio input and record audio
Bluetooth scan	Discover and pair nearby Bluetooth devices for apps with track and tracing features	Unauthorized access to device, unwanted monitoring of user’s behavior through track and tracing
System alert window	Enable the app to display over any other app without notifying the user	Displaying fraudulent ads, phishing, click-jacking, overlay windows, and preventing users from accessing the device by creating a persistent on-top screen
Bluetooth connect	Communicate with already-paired Bluetooth devices for apps with track and tracing features	Unauthorized access to device, unwanted monitoring of user’s behavior through track and tracing, unwanted passive or active data collection and analysis of user’s data,
Write calendar	Add appointments to device calendar, as scheduled with paramedics and physicians	Unauthorized access to delete, insert, or update user’s calendar
Bluetooth advertise	Make device discoverable to other Bluetooth devices for apps with track and tracing features	Unauthorized access to device, unwanted monitoring of user’s behavior through track and tracing
Read calendar	Read user’s calendar to schedule appointments for vaccination	Unauthorized access to user’s calendar data
Read contacts	Retrieve the name and phone number of individuals from device’s contact list for case interview for apps with track and trace features	Unauthorized access to read user’s contacts data
		Unauthorized access to user’s physical activity

(continued)

Table 3. Continued.

Permission	App functionality	Data privacy risk
Activity recognition	Detect user's step count or classify the user's physical activity	
Get accounts	Share digital vaccination information with user's contacts	Unauthorized access to user's list of accounts in the Accounts Service

Table 4. Checklist and rubric for privacy policies used to calculate privacy transparency index.

PTI Item	Score
Privacy (25 points)	
Does the app collect personally identifiable information?	Yes = 0; partial = 5[a]; no = 10
Does the privacy policy mention that the app can be used without entering identifiable information?	Yes[b] = 5; no = 0
Does the privacy policy mention that the app collects identifiable information such as full name, email, and phone number?	Yes or (N/A[c])[b] = 5; no = 0
Does the privacy policy mention that the app provides the option of a personal identification number, password, or log-in process to view and enter user data?	Yes or N/A[b] = 5; no = 0
Data management (50 points)	
Does the privacy policy explicitly state which type of data are processed?	Yes = 15; no = 0
Does the privacy policy contain a section on "how the app works" explicitly?	Yes = 5; no = 0
Does the privacy policy state that the app or server encrypts the entered data?	Yes = 10; no = 0
Does the privacy policy describe the process of data exchange and communication between server and phone-related to user-entered information?	Yes = 5; no = 0
Does the privacy policy state that the user information is stored on the phone or device?	Yes = 10; no = 0
Does the privacy policy mention data retention?	Yes = 5; no = 0
Legal framework (25 points)	
Does the privacy policy mention the GDPR[d]? If not, does the privacy policy mention other legislative framework?	Yes = 15; no = 0
Does the privacy policy state whether users can delete entered information?	Yes = 5; no = 0
Does the privacy policy state whether users can edit entered information?	Yes = 5; no = 0
	Grand Total: 100 points

[a] In this context, partial information is related to the use of location services only.
[b] Not applicable options for apps that do not collect personal or identifying information.
[c] N/A: not applicable.
[d] GDPR: General Data Protection Regulation.

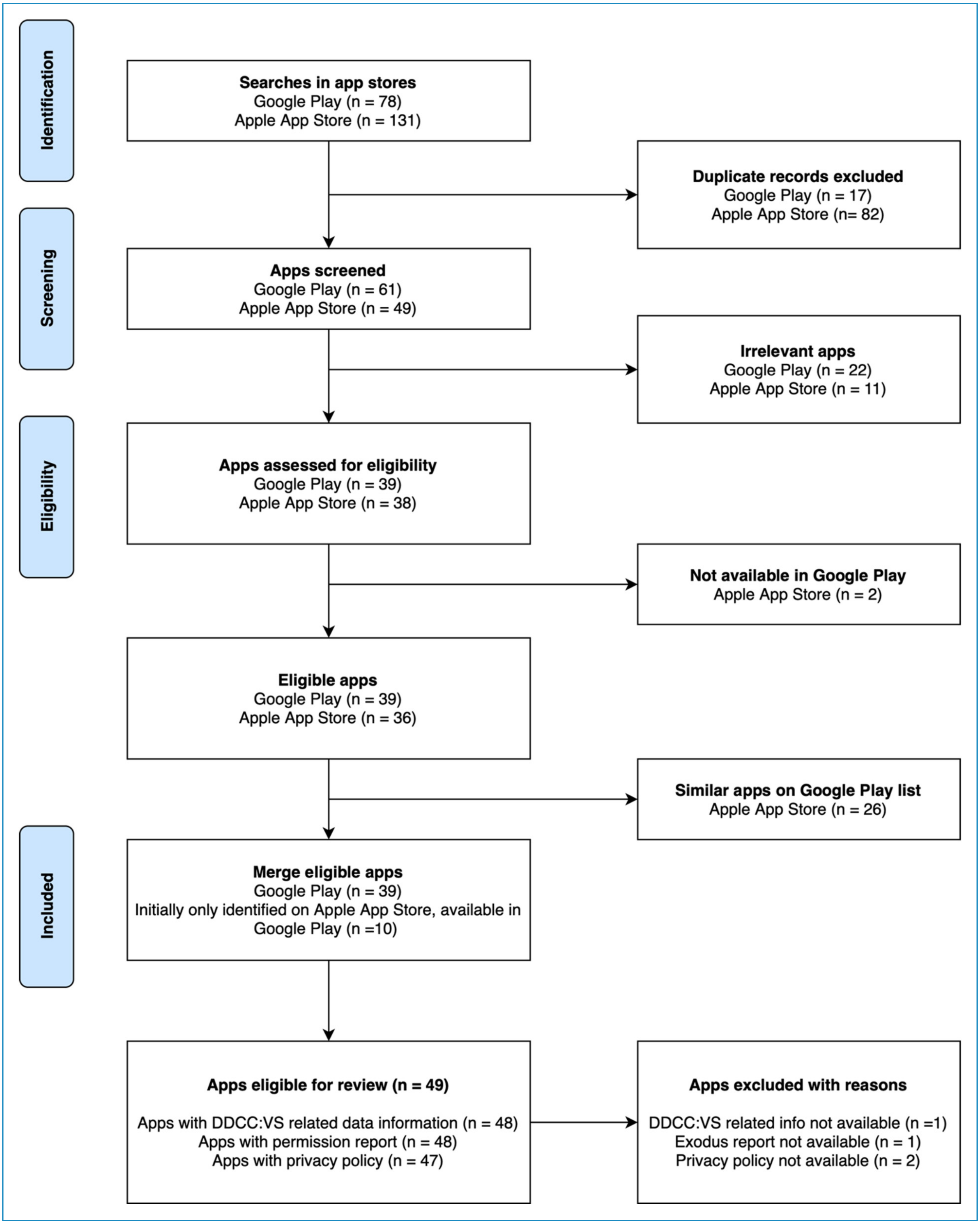
Identification
Screening
Eligibility
Included
Searches in app stores
Google Play (n = 78)
Apple App Store (n = 131)
Duplicate records excluded
Google Play (n = 17)
Apple App Store (n= 82)
Apps screened
Google Play (n = 61)
Apple App Store (n = 49)
Irrelevant apps
Google Play (n = 22)
Apple App Store (n = 11)
Apps assessed for eligibility
Google Play (n = 39)
Apple App Store (n = 38)
Not available in Google Play
Apple App Store (n = 2)
Eligible apps
Google Play (n = 39)
Apple App Store (n = 36)
Similar apps on Google Play list
Apple App Store (n = 26)
Merge eligible apps
Google Play (n = 39)
Initially only identified on Apple App Store, available in Google Play (n =10)
Apps eligible for review (n = 49)
Apps with DDCC:VS related data information (n = 48)
Apps with permission report (n = 48)
Apps with privacy policy (n = 47)
Apps excluded with reasons
DDCC:VS related info not available (n =1)
Exodus report not available (n = 1)
Privacy policy not available (n = 2)

Figure 1. App selection process.

available (47/49, 95.92%). The majority (39/49, 79.59%) of policies were written in English. A few (8/49, 16.33%) policies had to be translated from the original languages to English using Google Translate. The remaining (2/49, 4.08%) apps had no privacy policies. A comprehensive list of all 49 apps we identified is included in Appendix

1. This list contains links to the apps' Google Play and Apple App Store pages.

The 49 apps covered five types of areas (countries or regions, states or provinces, cities, and institutions in the network) in 32 countries spanning six continents. In order of the number of apps, they came from North America (18), Asia (16), Europe (10), South America (2), Africa (1), Australia (1), and one was not based on a geographical location. Figure 2 represents the world map of the DDCC: VS apps' global distribution; the size of the bubble illustrates the number of apps for each country.

The United States of America had the greatest number of apps (14/49, 28.57%) apps followed by Canada (4/49, 8.16%), the United Arab Emirates, and the United Kingdom (2/49, 4.08%).

The apps were mostly sponsored by governments (37/49, 75.51%), followed by private organizations (7/49, 14.29%) and nonprofit organizations (3/49, 6.12%). The least number of apps involved multiple stakeholders, including a consortium of governmental, private, and nonprofit organizations (2/49, 4.08%).

We found a significantly high positive correlation between the country-wide app total installs and the people vaccinated (Table 5) with at least one dose in the country ($r = 0.93$, $P = <.001$). These findings may indicate that digital vaccination certifications help boost COVID-19 vaccination rates.[19,22]

App characteristics

As of 3 March 2023, based on Google Play install categories, the 49 apps totaled 286,871,300 installs (5,854,516 on average), ranging from 100 to 100 million installs (Appendix 2). The most installed app was *Aarogya Setu*, developed by the Indian National Informatics Centre eGov Mobile Apps department, while the least installed app was *EarthMedGO* developed by United Nation Enterprise Apps. Half of the apps were installed between 100,000 and 1 million times (24/48, 50%), with one-third being installed more than 1 million times (16/48, 33.33%), and the remaining being installed <100,000 times (9/48, 18.75%).

The average app rating was 3.54 (SD0.79) on Google Play and 3.30 (SD0.92) on the Apple App Store. The median number of reviews was 14,662 (IQR83,649; range 6281–89,930) on Google Play and 71 (IQR704; range 25–729) on the Apple App Store.

Proof of COVID-19 vaccination

From the total 49 apps, 48 provided documentation that could be used for assessment (Appendix 3), including product site (22/48, 45.83%), documentation (14/48, 29.16%), government site (10/48, 20.83%), product store site (9/48, 18.75%), and privacy policies (5/48, 10.42%).

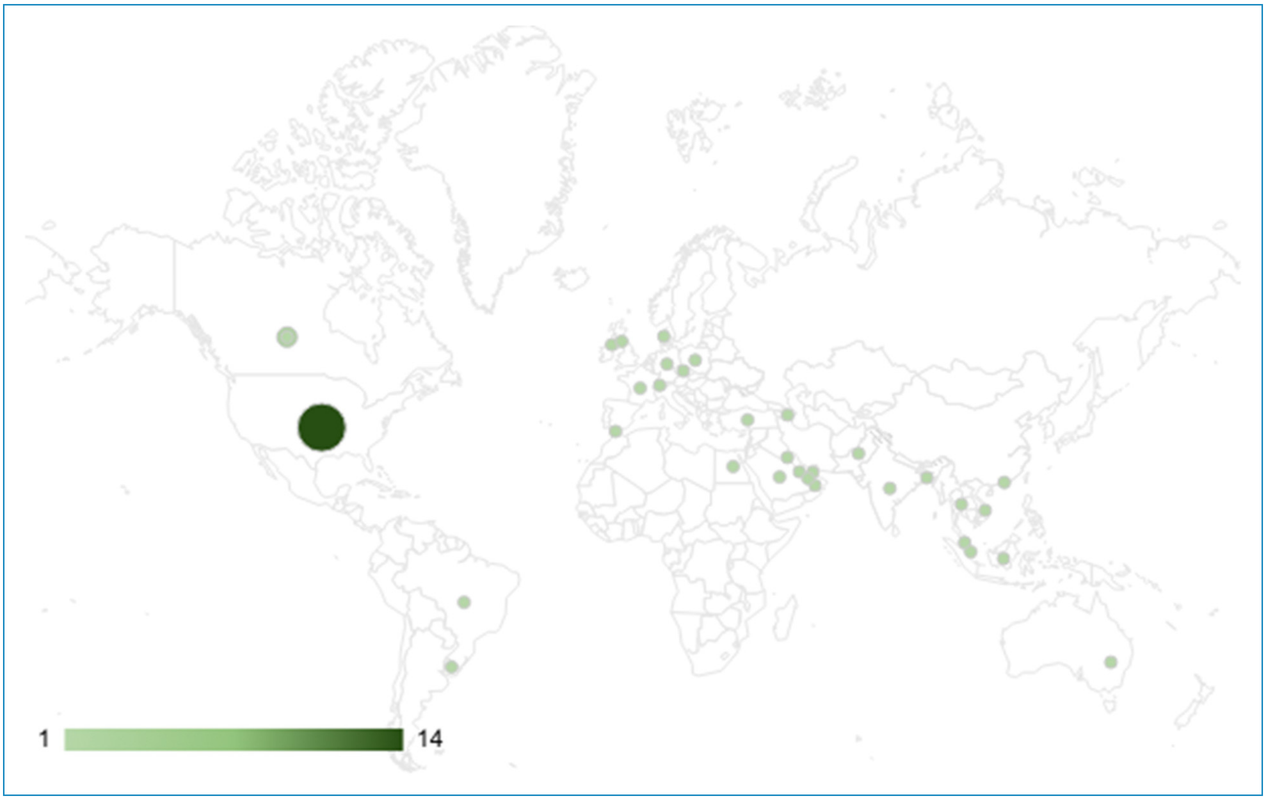

Figure 2. Geographic distribution of the DDCC:VS apps, clustered by country.

Table 5. Number of country-wide app installs and people vaccinated at least one dose (N = 28).

App name	Country	No. of installs	Last updated	People vaccinated at least one dose
e-Təbib	Azerbaijan	1,000,000	28 Aug 22	5,373,253
Surokkha	Bangladesh	5,000,000	1 Dec 22	148,052,616
ConecteSUS	Brazil	10,000,000	1 Dec 22	188,065,384
CANImmunize	Canada	100,000	2 Dec 22	34,358,732
ArriveCAN	Canada	5,000,000	1 Dec 22	34,358,732
Tečka	Czech Republic	1,000,000	1 Dec 22	6,974,217
Coronapas	Denmark	1,000,000	25 Nov 22	4,780,700
Egypt Health Passport	Egypt	100,000	27 Nov 22	53,646,548
TousAntiCovid	France	10,000,000	1 Dec 22	54,628,600
GHA COVID Pass	Gibraltar	10,000	21 Apr 22	42,074
LeaveHomeSafe	Hong Kong	1,000,000	1 Dec 22	6,900,553
Aarogya Setu	India	100,000,000	1 Dec 22	1,027,050,053
PeduliLindungi	Indonesia	50,000,000	28 Aug 22	203,435,374
Immune	Kuwait	1,000,000	28 Nov 22	3,453,545
MySejahtera	Malaysia	10,000,000	1 Dec 22	28,120,598
Tarassud +	Oman	1,000,000	25 Oct 22	3,257,365
Pak Vaccination Pass	Pakistan	500,000	30 Nov 22	139,628,133
mojeIKP	Poland	1,000,000	1 Dec 22	22,828,328
EHTERAZ	Qatar	5,000,000	27 Nov 22	2,849,216
Tawakkalna (Covid-19 KSA)	Saudi Arabia	10,000,000	28 Feb 22	25,960,748
TraceTogether	Singapore	1,000,000	1 Dec 22	5,151,095
COVID Certificate	Switzerland	5,000,000	1 Dec 22	6,094,838
หมอพร้อม	Thailand	10,000,000	30 Sep 22	57,005,497
Life Fits Home	Turkey	10,000,000	22 Nov 22	57,941,051
Alhosn	UAE	10,000,000	20 Jun 22	9,991,089
NHS App	United Kingdom	10,000,000	11 Sep 22	53,813,491
Coronavirus UY	Uruguay	1,000,000	1 Dec 22	3,005,033
PC-Covid Viet Nam	Vietnam	10,000,000	1 Dec 22	90,156,999

Two apps met all the nine required data, *NHS App* and *TraceTogether*. Most apps (36/48, 75.00%) included more than half of the required data, while few apps (4/48, 8.33%) included only two data. Of all 18 data (required and optional), *COVID Certificate*, *NHS App*, and *TraceTogether* included the most with 13 data. On average, apps included 6.31 (SD 1.99) required data or 70.14% (SD 22.12%) in percentage, and 8.98 (SD 3.00) overall data in their apps.

Nearly all the apps included *Name* (47/48, 97.92%), *Date of Vaccination* (44/48, 91.67%), *Vaccine Brand* (43/48, 89.58%), *Dose Number* (42/48, 87.5%), and *Date of Birth* (41/48, 85.42%). However, only about half contained *Vaccine Manufacturer or Vaccine Market Authorization Holder* (25/48, 52.08%), *Vaccine or Prophylaxis* (24/48, 50.00%), and *Vaccine Batch Number* (20/48, 41.67%). The least required data listed by the apps was *Country of Vaccination* (17/48, 35.42%). Regarding optional data, *Unique Identifier* (36/48, 75.00%) and *Administering Center* (31/48, 64.58%) were often included.

Data privacy

Across 48 apps with extractable privacy risk data (permission and tracker data), there were 80 unique data privacy risks (61 normal risks and 19 dangerous risks), and 28 unique trackers (Appendix 4). Figure 3 shows that, on average, apps had 14.75 (minimum 2, maximum 37) normal data privacy risks and 4.04 (minimum 0, maximum 12) dangerous risks. In general, the higher the data privacy risk, the higher the dangerous risk.

Figure 4 provides, for each of the 49 apps, detailed information on the identified data privacy risks and threats.

Figure 5 quantifies the dangerous permissions; 45 out of the 49 apps have at least one dangerous permission.

Permission to use *INTERNET* was the most frequent normal data privacy risk (47/48, 97.92%) and *CAMERA* (41/48, 85.58%) among the dangerous data privacy risks. Each app collected 14.75 data access permissions on average (IQR10, range 9–19), with the proportion of dangerous data privacy risks being 27% (IQR17%, range 17%–34%). Two apps (2/48, 4.17%) reported 12 dangerous data privacy risks (*DHA* and *United Airlines*), and the remaining (3/48, 6.25%) did not create dangerous data privacy risks.

On trackers, *Google Firebase Analytics* (31/48, 64.58%) was the most used followed by *Google CrashLytics* (18/48, 37.50%). While some of the apps (13/48, 27.08%) did not use any trackers, one utilized the most trackers (*United Airlines*, nine trackers), followed by other apps (3/48, 6.25%) that used six trackers (*CLEAR, e-Tabib, CANImmunize*). The apps used an average of 1.92 trackers (IQR 2.5, range 0.5–3).

On average, PARS was 28.58 (IQR 23.25, range 15–38.25). Of the 48 apps, *Surokkha* scored the lowest data privacy risk with 2, and *United Airlines* scored the highest data privacy risk with 87. Most apps had PARS <=50 (44/48, 91.67%).

Privacy policies

Forty-seven of the 49 apps had privacy policies (Appendix 5).

Regarding readability, the privacy documents required a median grade level of 14 (IQR 2.6, range 13–15.6). *NYC COVID SAFE* and *NHS App* had the lowest grade level of readability of grade level 11. *Alhosn* required grade level 22, and the translated documents of *Coronavirus UY* had grade level 23.

Most privacy policies were *difficult to read* or *very difficult to read* (25/47, 53.19%; 14/47, 29.79%, respectively).

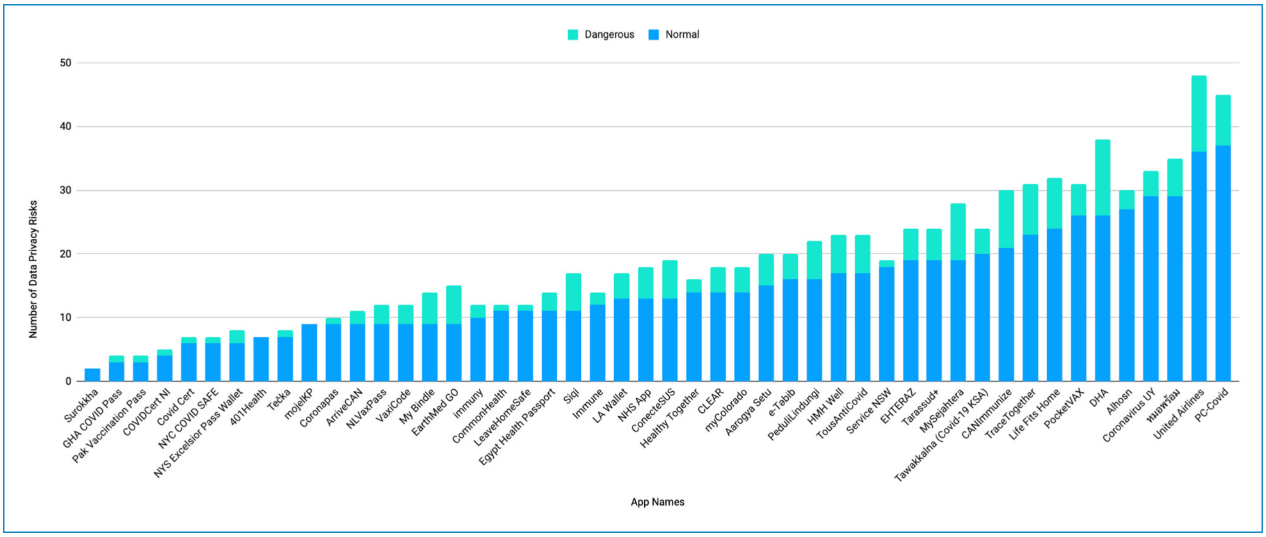

Figure 3. Distribution of the apps' number of normal and dangerous data privacy risks and threats, sorted from the least to the most (N = 48).

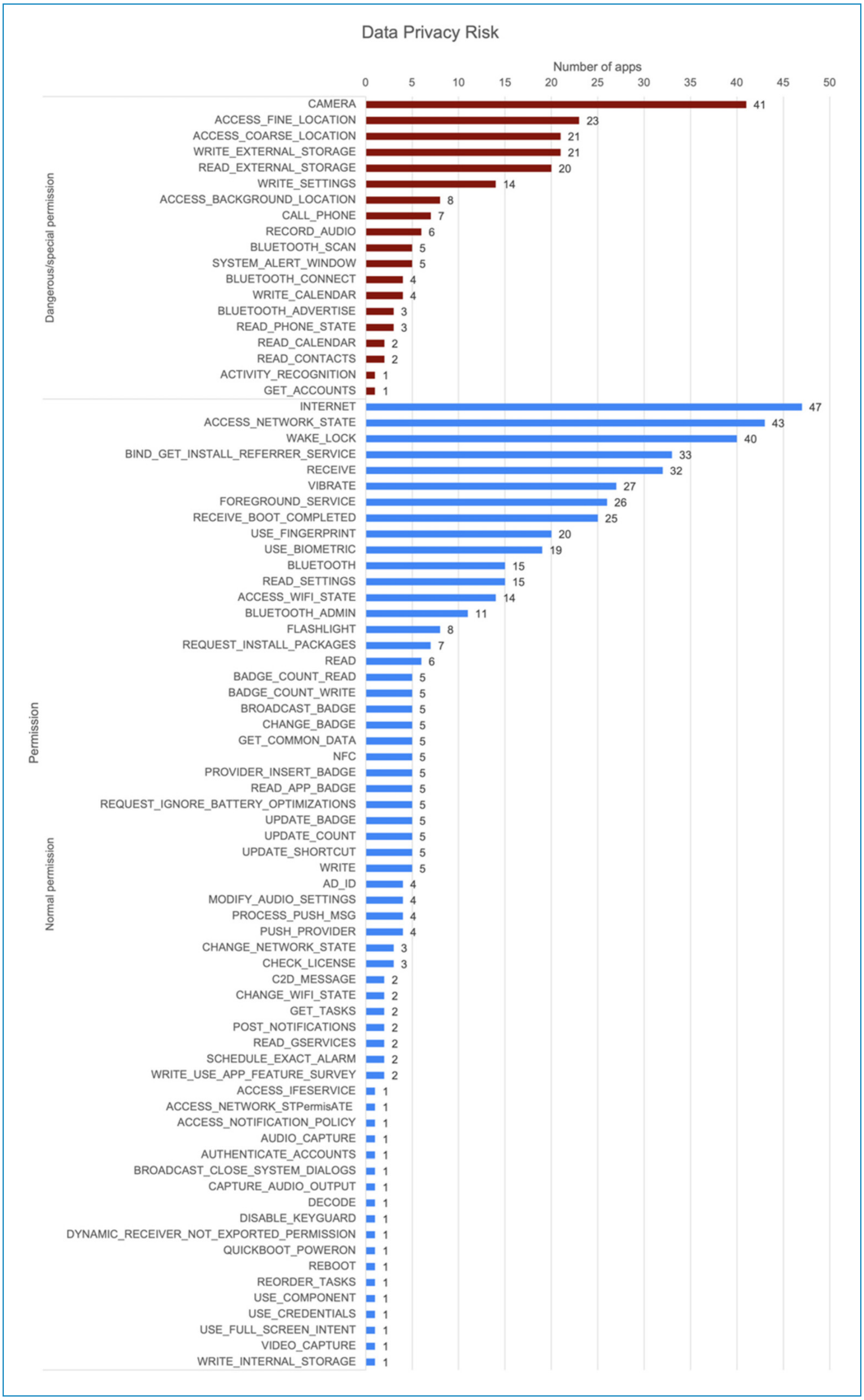

Figure 4. For each of the 49 studied apps, detailed information on identified data privacy risks and threats.

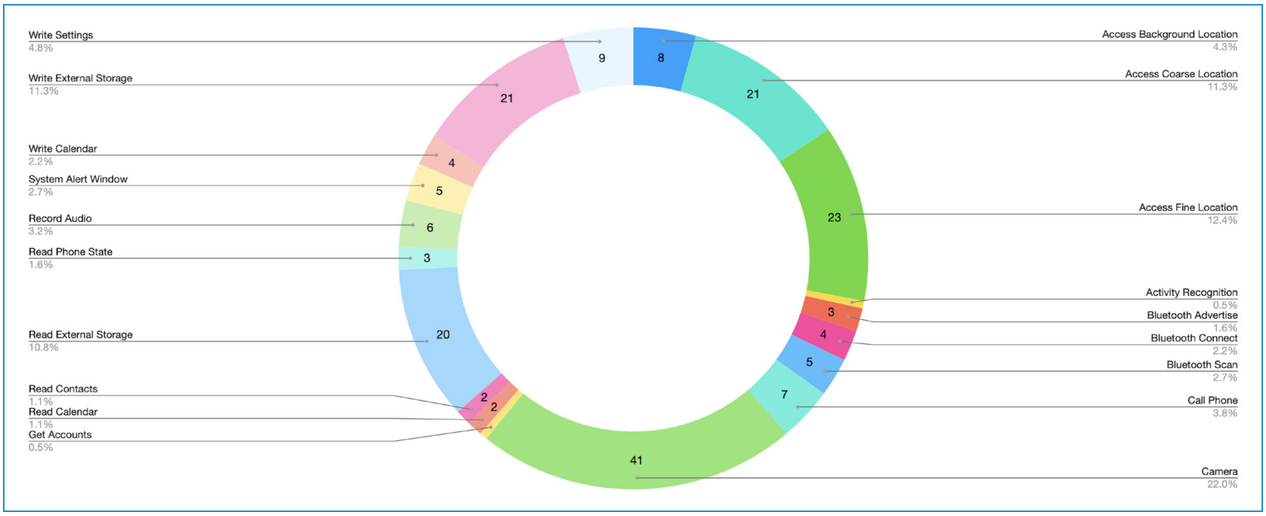

Figure 5. Distribution of apps broken down by type of dangerous data privacy risks (N = 45).

The remaining apps had privacy policies *fairly difficult to read* (8/47, 17.02%). No apps were within the *standard* or *average* reading level category.

In terms of PTI, *COVIDCert NI* achieved the highest average (75, SD 0.00), followed by *immuny* and *Tečka* (72.5, SD 3.54). *Tawakkalna* achieved the lowest average (22.5, SD 10.61), followed *by PC-Covid Viet Nam* (25, SD 0.00) and *Pak Vaccination Pass* (25, SD 7.07). The average PTI of all apps was 50.43 (SD 14.73; range 22.5–75).

Nine apps (9/47, 19.15%) had the least difference in PTI scoring between two reviewers (SD 0.00); 401Health, Aarogya Setu, Arrive CAN, ConecteSUS, COVIDCert NI, My Bindle, PC-Covid Viet Nam, PeduliLindungi, and หมอ พร้อม. CommonHealth and TraceTogether had the leading difference in PTI score (SD 21.21). The average standard deviation between the two reviewers' PTI scores was 7.07.

Table 6 shows the sample distribution according to the privacy policies rubric and the percent agreement (Pa) between two reviewers. Most privacy policies explicitly mentioned when the apps collect PII (44/47, 93.62%, Pa 87.23%) and when the apps collected identifiable information such as full name, email, and phone number (38/47, 80.85%, Pa 82.98%).

The least included items in the privacy policies were whether the privacy policies mentioned data retention (20.5/47, 43.62%, Pa 76.60%), the right of users to edit entered information (20/47, 42.55%, Pa 82.98%), and if the app can be used without entering identifiable information (0.5/47, 1.06%, Pa 97.87%).

The highest agreement was on whether the app could be used without entering PII (46/47, Pa 97.87%). Meanwhile, the item with the lowest agreement was whether the policy stated that the user information was stored on the phone or device (20/47, Pa 42.55%). The average observed agreement was 34.23 with a percent agreement of 72.83%.

Figure 6 shows that, on average, apps had aggregated WHO compliance, PTI, and PARS scores of 89 (minimum −23, maximum 152). *COVIDCert NI* was the top-performing app, while *Siqi* scored the lowest.

Discussion

To our knowledge, this is the first review of worldwide DDCC:VS apps. Our study identified 49 apps with COVID-19 digital vaccine certifications from 32 countries. Of those 49 apps, 48 had valid documentation that could be assessed for compliance with WHO DDCC:VS guidelines, 48 had Exodus report links to extract app data privacy risks, and 47 had privacy policies.

Based on our findings, we recommend the following best practices to develop COVID-19 apps with digital vaccination certifications:

- *Comply with WHO requirements for privacy and security for global interoperability.* Only two apps (2/48, 4.17%) contained all the required data. On average, apps fulfilled only about two-thirds (6.31/9, 70.14%) of the required data on the scenario. Adopting WHO standards for documenting COVID-19 vaccination status is expected to support interoperability between countries and the diverse needs of individuals worldwide.
- *Disclose data access purposes and risks to users' privacy to build trust.* From the list of dangerous permissions and risks presented in Table 3, we learned that most of the app permissions are unrelated to the functionality of digital vaccination certificate (e.g. access to fine location, call phone, Bluetooth scan) because

Table 6. Completed checklist of the PTI applied to 47 apps, averaged from two reviewers.

Domain, item, and score	Apps, n (%)
Privacy	
Does the app collect personally identifiable information?	Pa 87.23%
Yes = 0	44 (93.62)
Partial = 5[a]	0 (0.00)
No = 10	3 (6.38)
Does the privacy policy mention that the app can be used without entering identifiable information?	Pa 97.87%
Yes or N/A[b] = 5	0.5 (1.06)
No = 0	46.5 (98.94)
Does the privacy policy mention that the app collects identifiable information such as full name, email and phone number?	Pa 82.98%
Yes or N/A = 5	38 (80.85)
No = 0	9 (19.15)
Does the privacy policy mention that the app provides the option of a personal identification number, password, or log-in process to view and enter user data?	Pa 55.32%
Yes or N/A = 5	25.5 (54.26)
No = 0	21.5 (45.74)
Data management	
Does the privacy policy explicitly state which type of data is processed?	Pa 78.72%
Yes = 15	38 (80.85)
No = 0	9 (19.15)
Does the privacy policy contain a section on "how the app works" explicitly?	Pa 57.45%
Yes = 5	26 (55.32)
No = 0	21 (44.68)
Does the privacy policy state that the app or server encrypts the entered data?	Pa 63.83%
Yes = 10	28.5 (60.64)
No = 0	18.5 (39.36)
Does the privacy policy describe the process of data exchange and communication between server and phone-related to user-entered information?	Pa 57.45%

(continued)

Table 6. Continued.

Domain, item, and score	Apps, n (%)
Yes = 5	23 (48.94)
No = 0	24 (51.06)
Does the privacy policy state that the user information is stored on the phone or device?	Pa 42.55%
Yes = 10	23.5 (50)
No = 0	23.5 (50)
Does the privacy policy mention data retention?	Pa 76.60%
Yes = 5	20.5 (43.62)
No = 0	26.5 (56.38)
Legal framework	
Does the privacy policy mention the GDPR[c]? If not, does the privacy policy mention other legislative framework?	Pa 76.60%
Yes = 15	24.5 (52.13)
No = 0	22.5 (47.87)
Does the privacy policy state whether users can delete entered information?	Pa 87.23%
Yes = 5	23 (48.94)
No = 0	24 (51.06)
Does the privacy policy state whether users can edit entered information?	Pa 82.98%
Yes = 5	20 (42.55)
No = 0	27 (57.45)

[a] Partial score when the app used location services only.
[b] N/A: not applicable.
[c] GDPR: General Data Protection Regulation.

some apps are not specifically designed only as a DDCC:VS app. The most dangerous data privacy risk was the request to access the *CAMERA*. Some apps like *Aarogya Setu*, *DHA*, and *TraceTogether* specified in their privacy policies that the camera was used for scanning QR codes, supporting documents, or face authentication. However, other apps did not declare their reason for accessing the camera, such as *Alhosn* and *Service NSW*. As the most used tracker, *Google Firebase Analytics* enables data collection about app users, cookies, and similar technologies. *Firebase* supports the European Union's General Data Protection Regulation (GDPR) and United States' California Consumer Privacy Act (CCPA).[23,24] However, it is the app developers' responsibility to notify the users by disclosing details on how cookies, identifiers, and similar technologies are used and how users can opt out of the features.

- *Make privacy policies available to comply with app stores and regulations.* Most apps (47/49, 95.92%) have their privacy policy documents available. All apps submitted to the Apple and Google App Stores must comply with their privacy policies indicating how they collect, use, and share user's personal data and user's rights. In addition, apps must obey the privacy law of the geographical areas where the users are based, for instance, CCPA or GDPR.[23,24] There is a significant relationship between the readability of

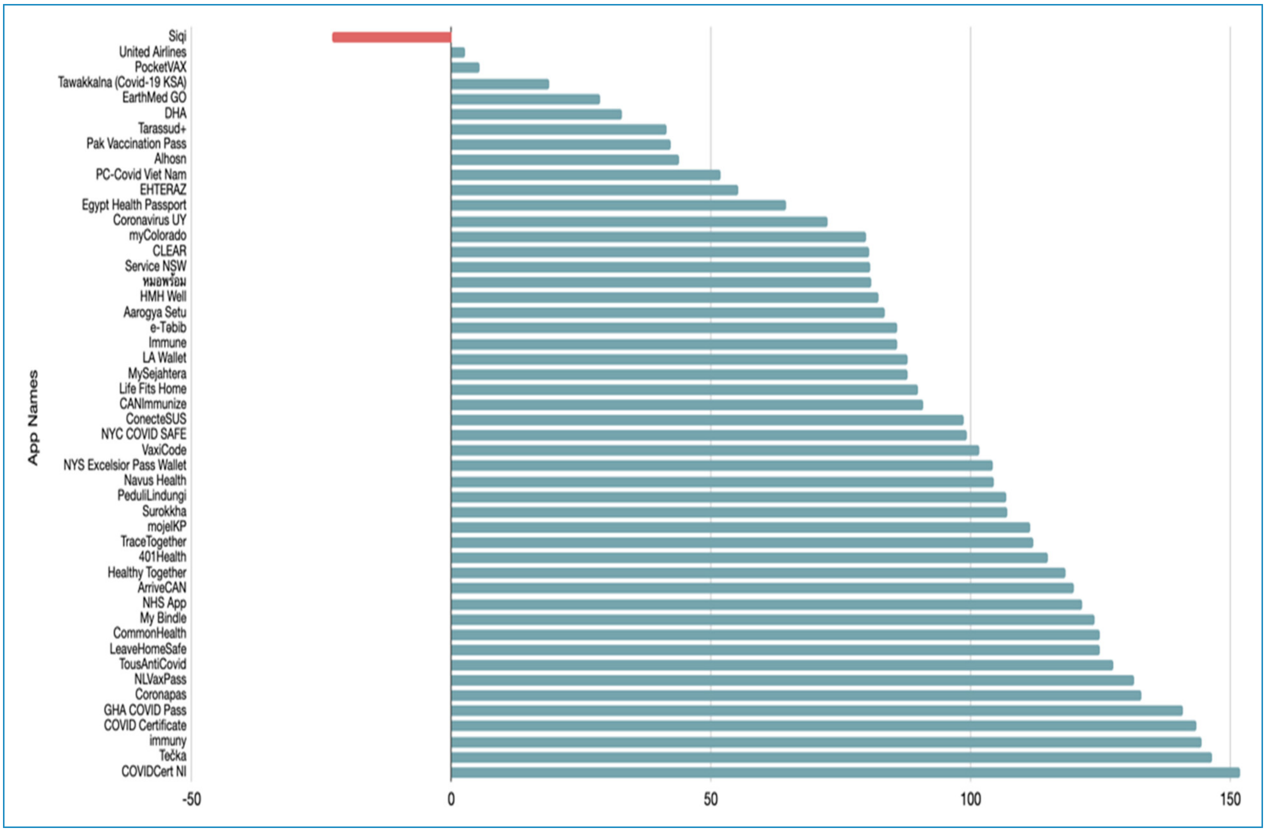

Figure 6. Apps and their aggregated scores for WHO compliance, PTI and PARS.

privacy policies and users' willingness to provide personal information, privacy concerns, and trust. Not having such documents in apps that record sensitive health data may concern users regarding developers' transparency and negligence.

- *Make privacy policies readable (sixth-grade level or less) to be inclusive:* The privacy policies of most apps (39/47, 82.98%) were difficult to read or very difficult to read. The lowest grade level of readability was grade level 11, and the average was grade level 14. Consistent with Sunyaev et al., our finding suggests that only university-level educated users could comprehend the information in the data privacy documents.[25] Complete transparency on data privacy rules and reading grade level six should be expected from apps that collect user information and use them for future reference.

Limitations

Unlike Android apps, iOS apps do not disclose information about permissions and trackers that could be used to assess data privacy risk. Our correlation analysis of vaccination uptake and number of app installs excluded apps not country-wide covering (21/49, 42.86%), and inferring causation would need further study considering potential confounding variables.

Our research adopted the PARS and PTI metrics developed by Bardus et al., which have not been extensively tested and are potentially prone to subjectivity and errors. We managed this challenge by incorporating multiple reviewers, cross-evaluation processes, and discussions to reach a consensus.[17] Additionally, we performed statistical analysis in PTI scoring to measure the disagreements between the two reviewers.

We did not check if the apps maintain/update the data privacy policies or if they comply with them. There are regulations governing the app's privacy policies to ensure that each privacy policy is easy to understand, is updated regularly, and informs customers of data that the app will collect (what the data will be used for, who will have access to the information, and why it is being collected). The most common regulation used in privacy policies to ensure the confidentiality of PII is GDPR as it covers 28 countries, but other regulations could cover one to two countries.

The mobile app market and the pandemic situation are dynamic. We presented an international snapshot of all available COVID-19 digital vaccination certificate apps as of 3 March 2023. Considering that we are still in a pandemic, the apps from the list could disappear or be modified, and new apps could emerge. Therefore, in the future, the existing apps from our database may have different digital vaccination certificate data, software permissions, and privacy policies.

Future work

Our study covered three of the ten variables expressed as relevant by the WHO to assess digital health solutions with objective, responsible, and transparent criteria. The remaining seven variables (oversight and regulation, interoperability, technical consideration, ease of use, ethical considerations, deployment considerations, and sustainability) were not explored. Additionally, the compliance of vaccination apps with health data sharing and privacy policies (such as HIPAA and GDPR) should have been studied.

Conclusion

Our review discovered a total 49 DDCC:VS apps. For those apps, we assessed their compliance with the WHO DDCC: VS Proof of Vaccination Scenario Requirements, their data privacy risk levels, and the readability and transparency of their privacy policies. As a result, we recommended app developers to: (1) comply with WHO requirements for privacy and security for global interoperability, (2) disclose data access purposes and risks to users' privacy to build trust, (3) make privacy policies available to comply with app stores and regulations, and (4) make privacy policies readable (sixth-grade level or less) to be inclusive.

Contributorship: The idea for this manuscript comes from IA. IA and SG contributed equally to data collection, analysis, and manuscript drafting. AG led the study design, project management, and manuscript preparation.

Ethics committee approval: This study did not involve human subjects and was exempted by the Arizona State University Institutional Review Board. No patient consent was required.

Guarantor: Adela Grando.

Declaration of conflicting interests: The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding: The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs: Isca Amanda https://orcid.org/0009-0008-4895-1143
Maria Adela Grando https://orcid.org/0000-0002-5769-8556

Supplemental material: Supplemental material for this article is available online.

References

1. WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020. Accessed January 28, 2024. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020
2. Coronavirus. Accessed January 28, 2024. https://historyofvaccines.org/diseases/coronavirus
3. Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance, 27 August 2021. Accessed January 28, 2024. https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1
4. How Private Is Your Digital Vaccine Record? Accessed January 28, 2024. https://news.bloomberglaw.com/privacy-and-data-security/how-private-is-your-digital-vaccine-record
5. Privacy Risk Management. ISACA. Accessed January 28, 2024. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/privacy-risk-management
6. PeduliLindungi: to care for and protect? | Association for Progressive Communications. Accessed January 28, 2024. https://www.apc.org/en/news/pedulilindungi-care-and-protect
7. Around 1 million people potentially affected by suspected breach in Indonesia's COVID-19 app: report | Healthcare IT News. Accessed January 28, 2024. https://www.healthcareitnews.com/news/asia/around-1-million-people-potentially-affected-suspected-breach-indonesias-covid-19-app
8. Report: Indonesian Government's Covid-19 App Accidentally Exposes Over 1 Million People in Massive Data Leak. vpnMentor. Accessed January 28, 2024. https://www.vpnmentor.com/blog/report-ehac-indonesia-leak/
9. Whittaker Z. A security bug in health app Docket exposed COVID-19 vaccine records. TechCrunch. Published October 27, 2021. Accessed January 28, 2024. https://techcrunch.com/2021/10/27/docket-vaccine-records-covid-security/
10. Balebako R, Schaub F, Adjerid I, et al. The impact of timing on the salience of smartphone app privacy notices. In: Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices. SPSM '15, 2015, pp.63–74. Association for Computing Machinery. doi:10.1145/2808117.2808119
11. Aydin A, Piorkowski D, Tripp O, et al. Visual configuration of mobile privacy policies. In: Proceedings of the 20th International Conference on Fundamental Approaches to Software Engineering - Volume 10202, 2017, pp.338–355. Springer-Verlag. doi:10.1007/978-3-662-54494-5_19
12. Schaub F, Balebako R, Durity AL, et al. A design space for effective privacy notices*. In: Selinger E, Polonetsky J and Tene O (eds) *The cambridge handbook of consumer privacy*. 1st ed. New York: Cambridge University Press, 2018, pp.365–393. doi:10.1017/9781316831960.021.
13. Balebako R, Jung J, Lu W, et al. "Little brothers watching you": raising awareness of data leaks on smartphones. In: Proceedings of the Ninth Symposium on Usable Privacy and Security, 2013, pp.1–11: ACM. doi:10.1145/2501604.2501616
14. Almuhimedi H, Schaub F, Sadeh N, et al. Your location has been shared 5,398 times! a field study on mobile app privacy nudging. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. CHI

'15, 2015, pp.787–796: Association for Computing Machinery. doi:10.1145/2702123.2702210

15. Howell B. Which countries are using COVID-19 vaccine passports? MoveHub. Published April 23, 2021. Accessed January 28, 2024. https://www.movehub.com/blog/countries-using-covid-passports/
16. Mbunge E, Fashoto S and Batani J. COVID-19 digital vaccination certificates and digital technologies: lessons from digital contact tracing apps. Published online March 16, 2021. doi:10.2139/ssrn.3805803
17. Bardus M, Al Daccache M, Maalouf N, et al. Data management and privacy policy of COVID-19 contact-tracing apps: systematic review and content analysis. *JMIR Mhealth Uhealth* 2022; 10: e35195.
18. Mathieu E, Ritchie H, Rodés-Guirao L, et al. Coronavirus pandemic (COVID-19). Our World in Data. Published online March 5, 2020. Accessed January 28, 2024. https://ourworldindata.org/covid-vaccinations
19. Vaccine Passports Help Boost Lagging Vaccination Rates | Vaccination | JAMA | JAMA Network. Accessed January 28, 2024. https://jamanetwork.com/journals/jama/fullarticle/2788129
20. Google Translate. Accessed January 28, 2024. https://translate.google.com/
21. Get your document's readability and level statistics - Microsoft Support. Accessed January 28, 2024. https://support.microsoft.com/en-us/office/get-your-document-s-readability-and-level-statistics-85b4969e-e80a-4777-8dd3-f7fc3c8b3fd2
22. Mills MC and Rüttenauer T. The effect of mandatory COVID-19 certificates on vaccine uptake: synthetic-control modelling of six countries. *The Lancet Public Health* 2022; 7: e15–e22.
23. General Data Protection Regulation (GDPR) – Official Legal Text. General Data Protection Regulation (GDPR). Accessed November 7, 2023. https://gdpr-info.eu/
24. California. California Online Privacy Protection Act. Accessed November 7, 2023. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC
25. Sunyaev A, Dehling T, Taylor PL, et al. Availability and quality of mobile health app privacy policies. *J Am Med Inform Assoc* 2015; 22: e28–e33.