



Health Data Regulation:

Lessons from COVID-19 Surveillance in Kenya and Uganda

June 2023

Introduction


As global interest in the regulation of health data picks pace, it is instructive to revisit how health data has been handled in some African countries in exercises involving the collection of large amounts of data. This examination is crucial to appreciate the key challenges faced in safeguarding the privacy and security of health-related data. In turn, this can provide pointers to the areas that require regulation and strengthening of practices.

This brief takes a look back at how personal data related to Coronavirus Disease 2019 (COVID-19) was collected and handled, and what lessons that experience offers for the future of health data regulation and governance. In particular, the brief reviews the experiences of Kenya and Uganda.

Emergency situations such as epidemics create an environment which can require the hasty collection and use of personal data. Indeed, Kenya and Uganda adopted various COVID-19 measures to facilitate disease surveillance and enforcement of Standard Operating Procedures (SOPs) by health and other authorities to combat the pandemic.

However, there were concerns about how data was collected, stored, and shared. Some measures related to tracking and monitoring people's movements, communications and health data by governments and private entities were deemed to have breached the right to privacy, lacked sufficient oversight, and did not respect data protection principles.¹

Regulations Governing COVID-19 Data Collection



In April 2020, Kenya issued the Public Health (Prevention, Control and Suppression of COVID-19) Rules, 2020 that provided for contact tracing, testing, isolation, and quarantine of suspected COVID-19 patients.² The Rules empowered health officials to enter and search premises for suspected cases.

Uganda's Public Health (Control of COVID-19) Rules, 2020 offered a legal basis for contact tracing. These Rules gave powers to a medical officer or a health inspector to enter any premises to search for COVID-19 cases or inquire whether there are cases of the coronavirus on the premises, and to order the quarantine or isolation of all contacts of suspected COVID-19 patients. Similarly, the Public Health (Prevention of COVID-19) (Requirements and Conditions of Entry into Uganda) Order, 2020 allowed for COVID-19 examination of arriving passengers at ports of entry.

¹ Resetting Digital Rights Amidst The Covid-19 Fallout, <https://cipesa.org/wp-content/uploads/2021/04/The-State-of-Internet-Freedom-in-Africa-2020-Report.pdf>

² Kenya's COVID-19 Measures and their Impact on Civic Space, <https://www.icnl.org/wp-content/uploads/Kenya-COVID-measures-FAQ.pdf>

Key COVID-19 Data Governance Issues

According to the World Health Organization (WHO), surveillance was critical to understanding the evolution of the virus, the risk factors for severe disease and the impact of vaccination and public health and social measures.³ In Uganda and Kenya, the aim of contact tracing and monitoring was to ensure that those exposed to the virus had limited interactions in public spaces and that they could be identified, quarantined and treated. However, the exercise registered data rights violations.

Safety and Security of COVID-19 Data: The data collection and conduct of health surveillance lacked sufficient oversight, safeguards, or transparency. Some of the apps deployed were not secure enough to host sensitive information, as they were developed by entities that lacked proper data governance frameworks and practices.⁴ The potential for data breaches was therefore high, with potential stigmatisation and other ramifications for COVID-19 infected individuals whose information circulated beyond health authorities.

Unenforced COVID-19 Data Collection Regulations: Both Kenya and Uganda had enacted data protection laws in 2019 that made it an offence to collect or process personal data in a manner that infringes on the right to privacy of an individual. However, there is no evidence that the data protection authorities in these countries monitored the enforcement of the COVID-19 data protection regulations.

In January 2021, Kenya's Office of the Data Protection Commissioner (ODPC) published a *Draft Guidance note on Access to Personal Data During the COVID-19 pandemic*, advising how technological apps and other services developed to tackle the pandemic may request access to personal data from government institutions or private entities to enable product development. There is no indication that the guidelines were enforced. In Uganda, the Personal Data Protection Office (PDPO) was not operationalised until August 2021 - deep into the enforcement of the country's disease surveillance measures. To-date, there is no indication that the Office had any oversight over the enforcement of COVID-19 Rules and the Order of 2020 in accordance with the data protection law.

Disregard for Data Protection Principles: Uganda's Data Protection and Privacy Act 2019 protects the privacy of individuals by regulating the collection and processing of personal information. Kenya's 2019 data protection law does likewise. Both laws provide for the rights of the persons whose data is collected. They also oblige data collectors and data processors to ensure the safety of the data and oblige them to be accountable to data subjects regarding how their data is collected, how it is stored, and for how long it is stored.

Unfortunately, some measures the countries adopted did not meet these principles. For example, Uganda handed motorcycle transporters (commonly known as boda bodas) the obligation to collect their customers' data and be responsible for its safe storage, without any guidance on how to do so, how long to keep the data, and where to take the data they collected.⁵ In Kenya, COVID-19 rules also mandated ill-equipped entities such as religious institutions and events managers to collect personal data including names, contact information, residential address and body temperature for contact tracing purposes.

Confidentiality Concerns: Uganda and Kenya's COVID-19 regulations were not explicit in providing for the confidentiality of personal data as well as the time-frame when the said data should be de-identified. This is unlike the case with *South Africa's Regulations* to address, prevent and combat the spread of COVID-19 which specifically provide for notification of data subjects (Section 11H16) and de-identification of data (Section 11H17).



³ Public health surveillance for COVID-19: interim guidance, <https://www.who.int/publications/i/item/WHO-2019-nCoV-SurveillanceGuidance-2022.2>

⁴ COVID-19 Data Governance in Kenya: Lessons for the Future, <https://cipesa.org/wp-content/files/COVID-19-Data-Governance-in-Kenya.pdf>

⁶ COVID-19 and Data Rights in Uganda, <https://cipesa.org/wp-content/files/documents/COVID-19-and-Data-Rights-in-Uganda-Report-.pdf>

De-identifying data in South Africa

Section 11H17: Within six weeks after the national state of disaster has lapsed or has been terminated—

- (a) the information on the COVID-19 Tracing Database shall be de-identified;
- (b) the de-identified information on the COVID-19 Tracing Database shall be retained and used only for research, study and teaching purposes;
- (c) all information on the COVID-19 Tracing Database which has not been de-identified shall be destroyed; and
- (d) the Director-General: Health shall file a report with the COVID-19 Designated Judge recording the steps taken in this regard, and the steps taken pursuant to subregulation (16).

In Uganda, there were *reports* of individuals using online platforms, mainly Facebook and Whatsapp, to share personal contact details of suspected COVID-19 infected individuals, some of whom were targeted with *physical attacks* and threatened with *eviction*. Most of the personal information had been collected by airlines and the Ministry of Health from the returnees and was assumed to be confidential.

Multiplicity of Unsupervised Apps: There was a rushed, haphazard and duplicative development and deployment of applications. The privacy credentials of these apps, many of which collected data without consent, were not assessed by regulators or other independent parties. Their data management protocols and privacy guarantees were not clearly stated. In Uganda such apps included geolocation tracing app *E-pass*, the *C-19 Mobile Contact Tracing App*, *Call the Clinic*, ICT Ministry *Funded COVID Apps*, and *COVID Tracer*. In Kenya, there was contact tracing and quarantine management app *Jitenge MOH Kenya*, the *Kenyatta University* contact tracing and case management app, *KoviTrace*, vaccination e-portal *ChanjoKenya*, and *mSafari* for public transport. An assessment of some of these applications shows that there were failures to incorporate privacy safeguards at the design stage (i.e. privacy by design) as these apps captured more personal information than was required for their stated purpose.⁶

Lack of Transparency: There was hardly any proactive accountability and transparency by private and public actors about the extent of data collected, methods used, number of apps that collected such data, and whether the data was destroyed when it was no longer necessary for the purpose for which it was collected. There was also no transparency on the nature of partnerships between government bodies and private apps/ data collectors. The lack of such transparency and audits means that *opportunity was lost* to identify the pitfalls to avoid and the good practices to build on in handling data in emergency situations such as that which was posed by COVID-19. The lack of proactive accountability is contrary to the principle which requires data controllers to implement and supervise verification procedures to ensure that the measures adopted not only exist on paper but are implemented and work in practice.⁷

Lessons for Health Data Regulation

In today's highly digitalised society, where large amounts of data are being collected and the capacity to process and manipulate data is high, guidelines on collecting and using health data are needed. Health data is profoundly sensitive and breach of privacy can cause significant harm to concerned individuals and even affect health outcomes. Such regulation should guide how data is collected, how and where it is stored, who can share or process it, and what they can do with the data.

According to the *Transform Health Coalition*, the current lack of agreed regulatory standards to govern the collection and use of health data creates uncertainty in the way health data can be used within countries and across borders. This, it adds, means that data is not being maximised for public good purposes such as research, innovation and health planning.

⁶ *Unseen Eyes, Unheard Stories: Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19*, <https://www.article19.org/wp-content/uploads/2021/04/ADRF-Surveillance-Report-1.pdf>

⁷ https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

The coalition, which has spearheaded the development of *health data principles*, argues that there is a need for improved governance of the collection and use of data through “common regulatory standards to harness the potential, and manage the risks, of health data sharing within and across borders, ensuring data is used for public good and prioritising equity, whilst protecting individual rights.”

In African countries, there are only baby steps on health data regulation, although several countries have developed digital strategies including for the health sector. Beyond having national policies and strategies on digital health, “it is imperative for countries in Africa to have regulatory standards and guidance that address key regulatory challenges affecting the use of health applications.”⁸

Some experts have proposed that, in developing those guidelines, African governments should balance the responsibility to protect personal health data with the importance and value of sharing vital health data across platforms and geographies.⁹ Given this reality and the experience of how COVID-19 data was handled, a few pointers can be made for African governments as they think about regulating health data:

- Develop clear and comprehensive privacy rights-respecting guidelines on health data through consultative processes that involve different private, civil society and public sector actors.
- Regional and global cooperation in devising the guidelines is key to share best practices and promote cross-country cooperation and harmonisation of regulations.
- The health data regulations should clearly and robustly embed all the high-level data protection *principles*. For health data specifically, it must only be processed for a period not longer than is necessary to achieve the intended purpose.
- The guidelines should provide for assessment by independent bodies of applications and systems that collect health data for their privacy / data protection credentials.
- The guidelines should include provisions on data collection, storage, sharing during pandemics and other health emergencies.
- Government, private companies and medical facilities should be transparent about what data they hold, who they share it with, how they process and store it, and who accesses it and for what purpose.
- Developers of health apps should embrace privacy by design when developing applications that collect, store or process health data. They should also have internal data governance policies that highlight the steps to ensure that the data they collect and process is secure.
- Establish accountability mechanisms for apps and health data collectors and ensure data protection authorities proactively enforce them.
- Government bodies should be transparent about all public–private partnerships they enter that entail data collection, storage and data sharing.
- The regulations should encourage data sharing and reuse at national level, as well as cross-border sharing but provide mechanisms for ensuring the integrity of data that is shared.
- Require health data collectors to have privacy policies written in plain language describing their data governance protocols and privacy credentials.
- The regulations should require data collectors and processors to implement appropriate, timely and effective measures to demonstrate compliance with personal data processing regulations.

⁸ Regulatory standards and guidance for the use of health applications for self-management in Africa: scoping review protocol, <https://bmjopen.bmj.com/content/12/2/e058067>

⁹ Health data privacy and data sharing are possible in Africa,

<https://www.zawya.com/en/press-release/africa-press-releases/health-data-privacy-and-data-sharing-are-possible-in-africa-mer2se1g>



Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

📍 Plot 6 Semawata Place (Off Semawata Road) Ntinda, Kampala

✉️ programmes@cipesa.org

🐦 @cipesaug 📘 facebook.com/cipesaug 🌐 LinkedIn/cipesa

🌐 www.cipesa.org