



# COVID-19 and Digital Rights

A Compendium on Health Surveillance Stories in Africa



# COVID-19 and Digital Rights

## A Compendium on Health Surveillance Stories in Africa

May 2021

Published by

**Paradigm Initiative**

Supported by

**The Open Society Initiative for West Africa**

Editors

**'Gbenga Sesan**, Executive Director, Paradigm Initiative.

**Thobekile Matimbe**, Community Manager, Paradigm Initiative.

Design and Layout

**Kenneth Oyeniyi**, Communications Assistant, Paradigm Initiative.



Creative Commons  
Attribution 4.0 International (CC BY 4.0)



PARADIGM  
INITIATIVE

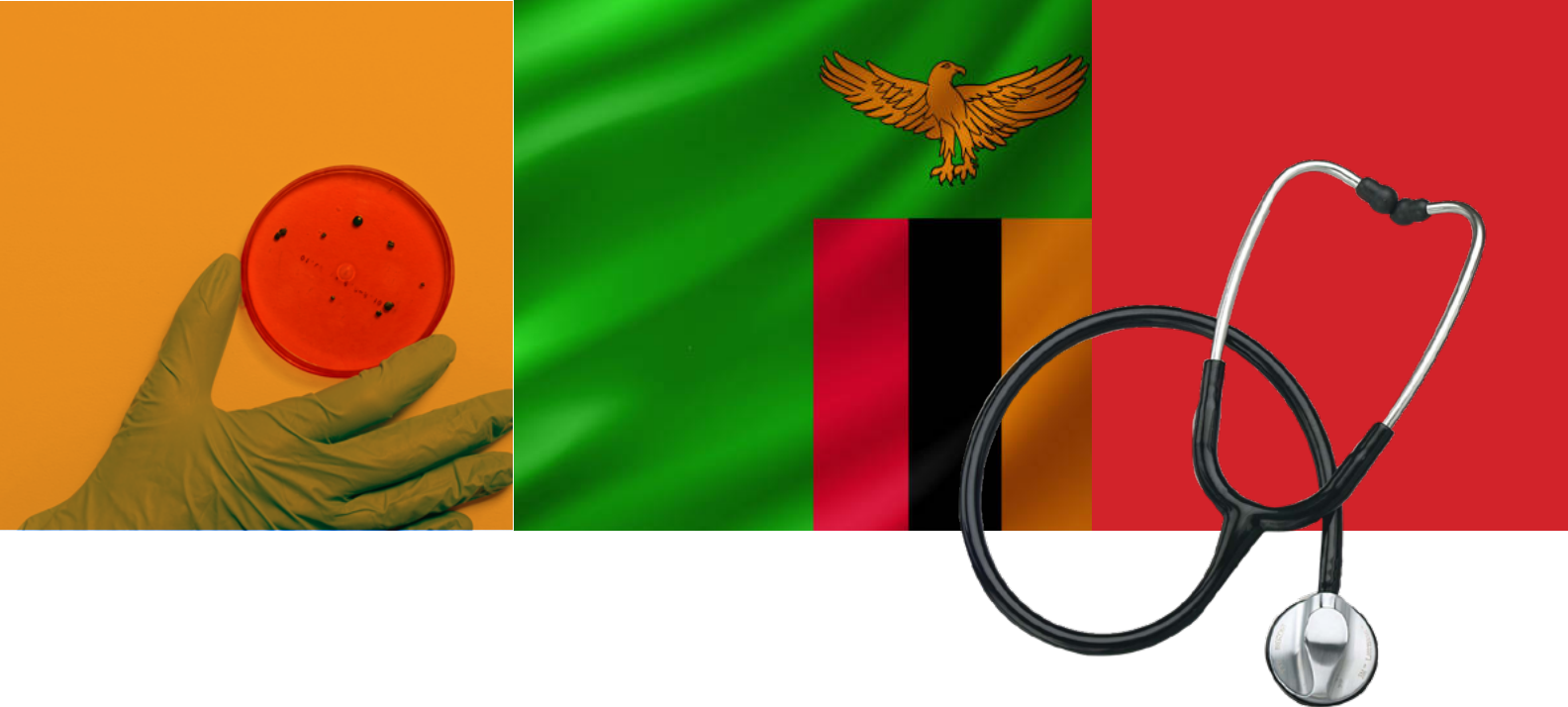


@ParadigmHQ

# Table of Contents

**Page**

<b>COVID-19 and the need for data privacy and protection regulations in Zambia</b>	<b>4</b>
<b>Covid-19 Digital Contact Tracing: Lessons From a Nigerian Experience</b>	<b>6</b>
<b>COVID-19: What turned my life upside down</b>	<b>8</b>
<b>The threat to data privacy in Kenya in the time of COVID-19</b>	<b>10</b>
<b>Safe-guarding Kenyans' data amidst a pandemic</b>	<b>12</b>
<b>TogoSafe application's data grab</b>	<b>14</b>
<b>The looming threat to data privacy for Nigerians in a pandemic</b>	<b>16</b>
<b>COVID-19: Between personal data breaches and disinformation in Cameroon</b>	<b>18</b>
<b>COVID-19 Case No.15: A Zimbabwean victim of misinformation</b>	<b>20</b>
<b>Protecting the privacy of Zimbabwean COVID-19 patients</b>	<b>22</b>



# COVID-19 and the need for data privacy and protection regulations in Zambia

Compiled by Bulanda Nkhowani

Zambia recorded its first two cases of COVID-19 in March 2020 and was one of the few countries in the region that partially kept its borders open. While most countries battled to find ways to understand, mitigate and stop the spread of the novel coronavirus, Zambian health professionals quickly took to a tried and tested method to prepare, surveil and respond to the looming threat. The Ministry of Health (MoH), through the Zambia National Public Health Institute (ZNPPI), implemented a multi-sectoral emergency response approach to fight COVID-19, an approach that had previously been used to fight reoccurring cholera outbreaks in the country. This involved activating the National Public Health Emergency Operations Centre (PHEOC) located at the ZNPPI and using a multi-sectoral Incident Management System (IMS) approach, supplemented by a dedicated call centre to coordinate efforts.

"It all started with a slight tickle in my throat upon returning from a trip to a neighbouring country for business. At that time COVID-19 had just hit Zambia and there was a general panic across the country. I called the toll-free line where the person from the call centre enquired about my symptoms. They also took down my names, phone number, physical address, occupation, next of kin and information about where I had physically been to in the last few days as well as whom I had interacted with. The person appeared to be typing and capturing my responses on the other end, they ended by promising that I would receive help from a response team that had been dispatched to assist me and that I stay put within my house. I was very lucky to have contracted the virus at a time when response teams were very fast in responding. In no time they arrived at my premises. Sadly, I tested positive for the virus, although I was not exhibiting severe symptoms, I was admitted to the COVID-19 isolation ward," said Mutale, one of the earliest COVID-19 survivors.


Tamara's case on the other hand was different, "After experiencing high fever and a dry cough, I visited the nearest health facility to test for COVID-19. My suspicions were right, I tested positive for the virus. I was led to a room where a medical professional manually took down my personal identifying details and those that would be used to trace any individuals that I had been in contact

with. I read a lot about data rights so naturally, I was concerned about how my information would be stored, used and for how long it would be kept seeing as the medical professional was now entering it onto a paper that could easily be lost. Also, my consent was not sought when acquiring this data, however, when I enquired as to what it would be used for, I was assured that it was safe and that it would be used only for purposes of contact tracing and reporting. I was later advised to self-isolate at home for a period of 14 days. In those days I got phone calls from my case manager enquiring how I was faring on a daily basis until the end of my quarantine period. I am not sure what became of my personal information," she said.

Zambia, like many countries in sub-Saharan Africa, uses a mostly manual contact tracing approach aided slightly by mobile phones and computers to monitor, locate and contact existing and potential COVID-19 patients. While no contact tracing apps exist, all relevant COVID-19 data are captured into a national public health database which then raises concerns on the safety and security of personal health data that is captured, especially for public health emergencies. Other systems and networks exist, for example a network that acts as a communications hub for all emergency field agents involved in the front-line fight against COVID-19.

Amid this data collection and uncertainty on the personnel and protocols involved in accessing the database or principles governing data sharing or third party involvement in the development, supply and management of the database, Zambia continues to lack data protection and privacy laws. Similarly, in 2017, Zambia rolled out an e-health system to deliver digital health solutions, further raising questions on the capacity of public health data handlers to adhere to data protection and privacy ethics.

It is clear that data is key to solving current and future public health threats. The urgent need for enactment of human rights-respecting data protection and privacy regulation, that safeguard personal data and privacy of citizens like Mutale and Tamara, is also more apparent. This need includes frameworks that oversee implementation of best practice policies on the capture, storage, management, transfer or retention of data on information systems. Furthermore, there is a strong need to build the capacity of health professionals and third parties' obligations when handling sensitive data. Citizen awareness is also critical in ensuring that the correct policies and protocols are implemented and that individuals' rights are not infringed upon.



Amid this data collection and uncertainty on the personnel and protocols involved in accessing the database or principles governing data sharing or third party involvement in the development, supply and management of the database, Zambia continues to lack data protection and privacy laws.





# Covid-19 Digital Contact Tracing: Lessons From a Nigerian Experience

Compiled by Adeboye Adegoke, with support from Temitope Opeloyeru

Much of our lives now revolve around the use of technology, which makes our work easier and faster, but technology is never a substitute for the quality of work required in its application.

In the wake of the COVID-19 pandemic, the world looked towards technology for succor as different stakeholders were working to stem the tide of the pandemic, to protect lives and revive the global economy. While the virus was spreading rapidly in 2020 with no effective antiviral therapy or vaccine, the world focused on managing the pandemic by containment. It is therefore understandable that technology was considered useful to facilitate pandemic containment strategy. Google and Apple, two of the world's leading technology companies, [announced a partnership](#) on COVID-19 contact tracing technology and were quick to [assure privacy protection](#) in their proposed rollout, affirming that user privacy and security are central to the design. There is [documented evidence](#) of [privacy protection](#) in the adoption of contact tracing applications in managing COVID-19 by European governments. Those efforts may have contributed to the eventual flattening of their incidence curves, despite challenges with low adoption, and privacy and security concerns.

In Nigeria, like many African countries, the government [announced lockdowns](#), [proposed the use of mobile data for COVID-19 surveillance](#), [introduced new legislation](#), and more. Notably, there was news of the development of digital contact tracing applications by both [State](#) and [non-state actors](#). These are measures with clear implications for digital rights, particularly the right to privacy. In order to understand the extent to which contact tracing measures were deployed by the Nigerian government, I carried out a survey to provide much-needed insight. This article is centered on stories from key informants who are either health professionals or COVID-19 survivors in Abuja, Nigeria.

Dr. Olajumoke Precious works for the Nigeria Center for Disease Control (NCDC) in Abuja. She has never tested positive for the virus but she interacts with patients. Her description of the contact tracing measure employed by NCDC is completely manual. She recognises that contact tracing is for surveillance, which involves identification, listing, and following up on certain persons who may have had contact or been in the immediate vicinity of the infected person. According to her:

"We do this by interrogating the activities of the case, or activities and roles of the people around the case, since the onset of symptoms. We also probe for places visited within 2-14 days prior to the onset of symptoms. We extract contact information like where the person lives, people around them, the family of the carrier and in cases where the person is dead, we visit the health facilities where the deceased was admitted before he or she died".

From a survivors' perspective, Joseph Nikoro, a multi-level marketer and farmer, provided the phone numbers of people he remembered he came in contact with, to health officials, and they told him to call them to ask if they have come in contact with any other persons. Available evidence clearly shows that technology was barely leveraged in all of these measures despite the hype around the efficacy of contact tracing measures, including digital contact tracing methods, and evidence that such apps were introduced in Nigeria.

Looking at the digital rights landscape in Nigeria, it is worrying to see the application of similar digital tracing technology during protests such as the October 2020 #EndSARS protest. While the Nigerian government struggles to demonstrate the effectiveness of the application of technology to fight criminality, terrorism, or stem the tide of a pandemic that represents an existential threat to humanity - which are the reasons usually avowed for buying these technologies - it has never failed to apply these technologies in targeting human rights defenders, critics and protesters. The Nigerian government's failure to trace bandits and terrorists, who are at the epicenter of the country's security challenges, remains a mystery despite huge investments in surveillance technologies. The sum of 9 billion naira (US\$22.8 million) was budgeted in 2020 for surveillance-related activities and equipment.

The swiftness with which government critics and protesters are digitally traced and arrested gives a clear indication of the danger of giving a government that has a history of clamping down on dissenting voices more intrusive power to further sinister objectives. These technologies barely serve legitimate purposes other than being a tool for intimidation and harassment of those who hold dissenting opinions. Eromosele Adene is still [facing trial](#) after being [tracked](#), arrested, and charged for his involvement in the #EndSARS protests. Salihu Tanko Yakasai was tracked, [arrested](#), and [sacked](#) for [criticising](#) the President's handling of security issues in the country in a series of tweets, in which he [asked the President to resign](#).

Technology is not a magic wand and is more likely to be used as a tool of intimidation by governments that have clampdown agendas. It is a tool that finds its most noble use in serving the objectives of diligent and competent actors so a governance structure that is bedeviled by incompetence and other anti-democratic tendencies will not effectively deploy surveillance tools for progressive uses. Rather, such governments will find technology tools useful in closing the civic space and shutting down opposition voices. This is why it is important for the technology and civic ecosystem to insist on a proper legislative framework, judicial accountability, and mandatory transparency in the application of surveillance technology.



..this is why it is important for the technology and civic ecosystem to insist on a proper legislative framework, judicial accountability, and mandatory transparency in the application of surveillance technology.



# COVID-19: What turned my life upside down

Compiled by Rigobert Kenmogne

In April 2020, when my aunt, Suzanne, went to the Djoungolo Health Center, in the city of Yaoundé, she did not know that she was going to experience some moving moments in her life. 50 years old, she went to the Health Center for a COVID-19 test. Four days, Suzanne had been reluctant to go to a Health Center for the test. Reassured to have made the right choice, under the advice of her cousin, she finally decides to go there one morning. Once in the Health Center, she is shy, because she has already started developing seizures after a few days of her onset of cough, external signs of a potential COVID-19 contamination.

Once at the Health Center, those in charge of the service will make arrangements to take the necessary samples. But the service is slow, due to many patients who want to know their health situation. In addition, the test kits are not in great numbers; the service is saturated; the cousin comforts Suzanne and they wait. Around the middle of the day, Suzanne gets her results, as the signs indicate her status is positive. She is visibly in shock and fears losing her life. Suzanne becomes blade, bruised and lives into silence for a few minutes. She was probably wondering if she could live with this contamination that is so scary. Suzanne must begin quarantine immediately. "Madam, your result is positive, you must go into quarantine, everything will be better with care" indicates a person in charge of the Center. She holds her breath and listens to the doctors' instructions. To avoid any outbreak of the disease, Suzanne's cousin must also be tested. She does not refuse. Fortunately, her status is negative, she has not contracted the disease, but the barrier measures, distancing and quarantine are necessary for her.

A week after the start of treatment in quarantine, Suzanne discovers that her COVID-19 status with her photos and those of other infected people in the Health Center are published on social media, in particular the Facebook and WhatsApp platforms. She was deeply disappointed, upset and lost a lot of weight in a few days. This situation caused other illnesses in her life context. Fortunately, she survived these difficult situations.




According to a young influencer who worked with Plan International-Cameroon, " Suzanne went into a rage when she saw her information online, which in fact made her situation worse". Suzanne confided that she was back in her forties thanks to the support of plan International and the work of young influencers of the organization and partners. As in similar cases, as part of its activities, Plan International, sensitized populations on the dangers of COVID-19 by distributing protection kits. Advice was given to Suzanne to help her health balance her moral. Campaigns on the ethical responsibility of physicians have also been initiated directly in targeted health centres or on social media.

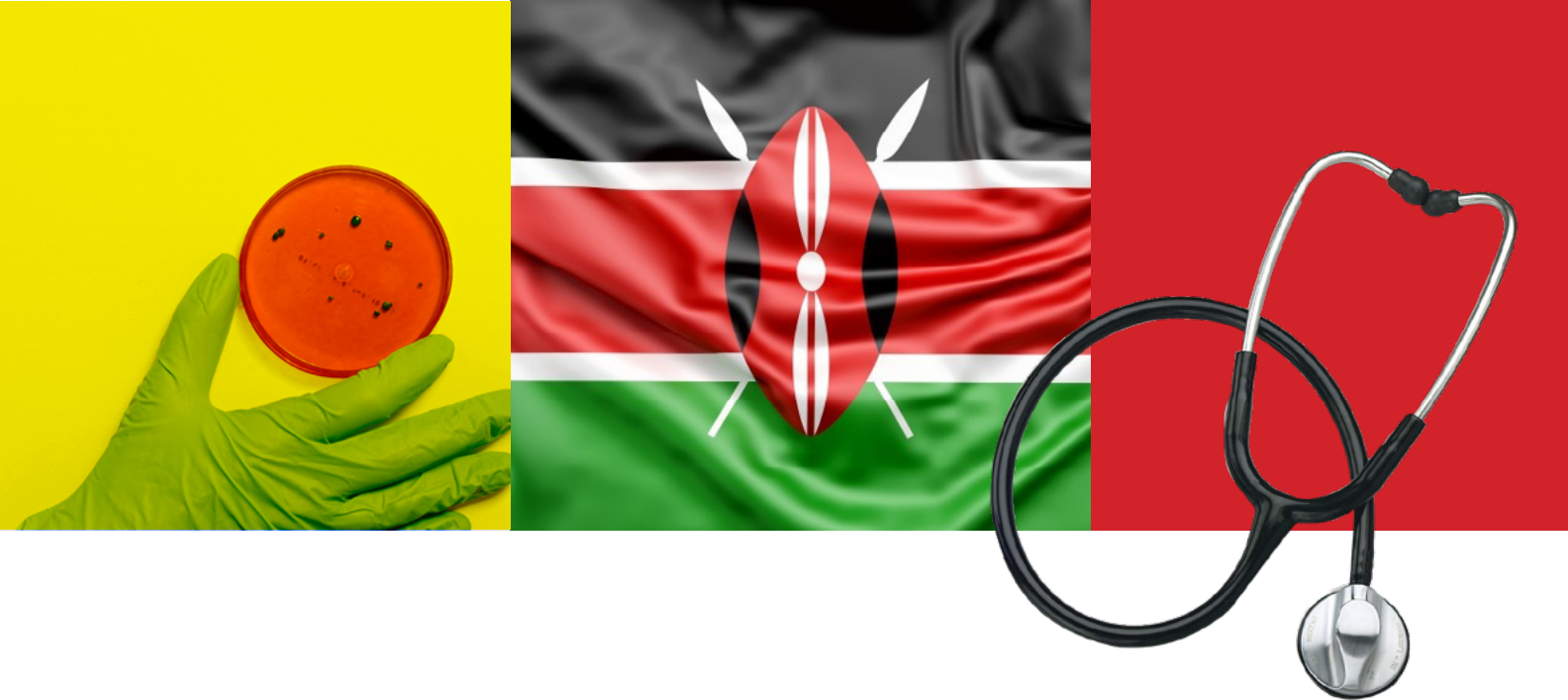
Since March 2020, at the start of the crisis, more than 10 cases of personal data breaches have been reported to Plan International through the activities of young influencers. More women than men have complained about posting their health status on social media.

On the prospects of protecting personal data and limiting violations as it has been for Suzanne and many others, the young influencer recommends: " we must adopt a law on the protection of personal data, make Internet users aware of the notion of personal data, encourage Internet users to read the confidentiality policies of social network companies, and draft and make available to the public a personal data protection charter for better impregnation ".

Plan International works in 4 areas: health, education, protection and defense of the rights of vulnerable people. The actions of the organization in raising awareness against the spread of COVID-19 and its impact on populations have been significant. For more information on Plan International, please visit <https://plan-international.org/>



we must adopt a law on the protection of personal data, make Internet users aware of the notion of personal data, encourage Internet users to read the confidentiality policies of social network companies, and draft and make available to the public a personal data protection charter for better impregnation



# The threat to data privacy in Kenya in the time of COVID-19

Compiled by Ekai Nabenyio

Even though the COVID-19 pandemic is global, the development and implementation of contact tracing has taken place only on national levels. At the onset of the COVID-19 pandemic, different methods were used by the Kenyan government to contain the spread of the pandemic. This included a mandatory quarantine order for all persons travelling into Kenya. Chali Baluu (name changed), a Kenyan citizen, reported human rights violations to the Kenya Human Rights Commission, complaining that his communication devices, specifically his mobile phones, were being monitored by government authorities. Numerous incidents were also reported on the State's tapping of phones and eavesdropping on private communications. Additionally, as a COVID-19 patient, Chali Baluu indicated to the Kenya Human Rights Commission (KHRC) that while placed under mandatory quarantine at Jomo Kenyatta International Airport in Nairobi, in compliance with the government directive, they were placed under 24/7 surveillance.

The challenge faced by the KHRC in monitoring the veracity or otherwise of these violations included the fact that it was not easy to prove monitoring of communication devices despite the seriousness of the allegations made. Individuals reported incidents to the KHRC in which they were placed under mandatory quarantine for periods more than the stated 14 days. This meant more surveillance for longer or indefinite periods. Further, the fact that staff of KHRC worked virtually meant that they received and handled these reports of violations virtually. This affected the credibility that is easier to prove during face to face communication. It also means that some cases of those less tech-savvy victims that would have otherwise paid a visit to the offices of the Commission may have gone unreported. Journalists that attempted to relay the information on COVID-19 human rights violations to the general public were often arrested as surveillance was extended to media houses, and vandalism was reported. The Media Council of Kenya did raise a complaint against this violation which essentially violated the right to access information guaranteed under the Constitution of Kenya, 2010. Article 35 (1) of the Constitution of Kenya states as follows:

Every citizen has the right of access to--

(a) information held by the State; and

(b) information held by another person and required for the exercise or protection of any right or fundamental freedom.

(2) Every person has the right to the correction or deletion of untrue or misleading information that affects the person.

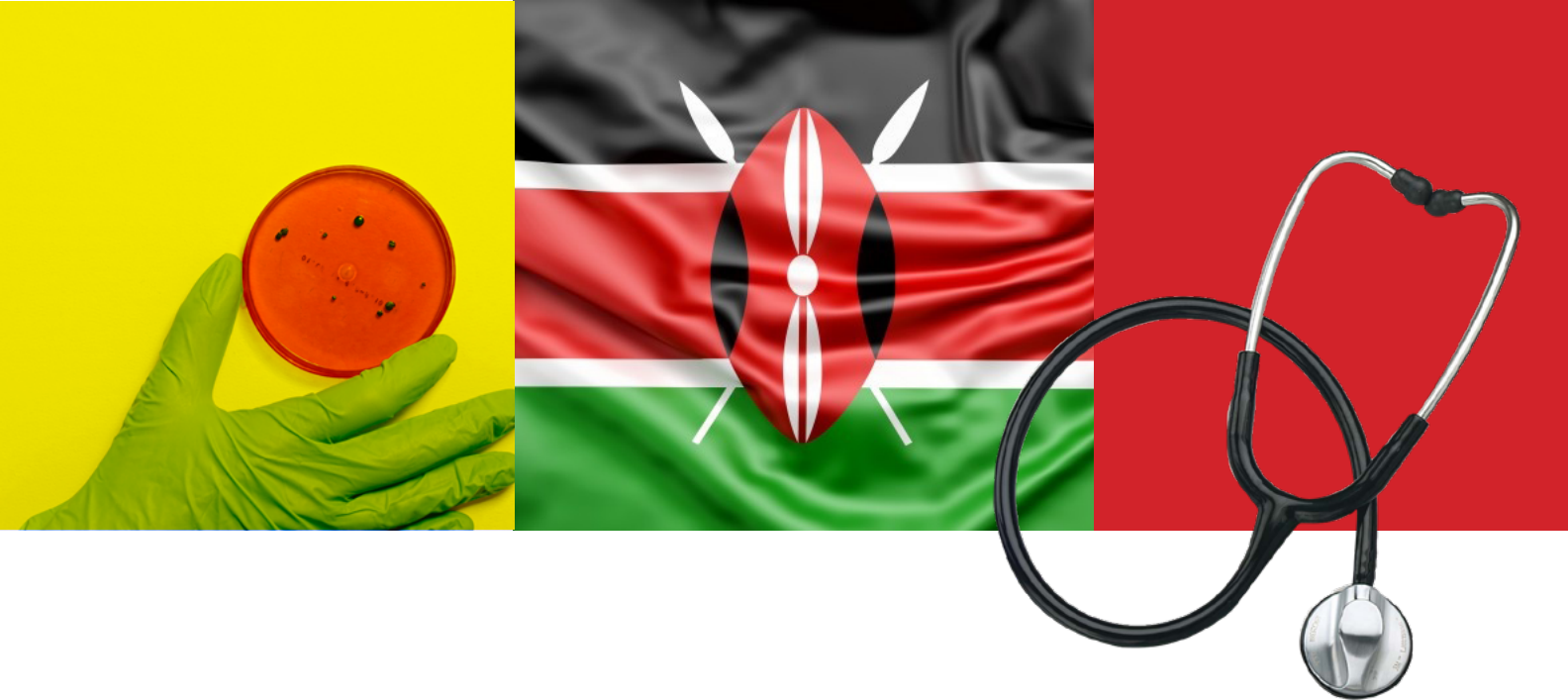
(3) The State shall publish and publicize any important information affecting the nation.

Regional and international human rights instruments such as The Declaration of Principles of Freedom of Expression and Access to Information in Africa demand that for any restriction on access to information held by public authorities to be allowed by law, it must have a legitimate aim, be necessary, proportionate to the aim of safeguarding public health, and must also be restricted to only the existence of the crisis. This means that any limitations of human rights should be justified. Information accessibility is a key component of the right to health and countries such as Kenya are urged to comply. When officials do not publish health information proactively, populations suffer adverse health impacts and cannot fully enjoy their right to health as guaranteed. Kenya needs to be open and transparent, responsive and accountable to the citizens in the fight against COVID-19.

The reduction in the public's right to know about the activities of their governments is counter-productive to the effort in combating the COVID-19 outbreak. The right to information is crucial for ensuring public awareness and trust, fighting misinformation, ensuring accountability as well as developing and monitoring implementation of public policies aimed at solving the crisis. It is crucial that the right to information is maintained during the emergency as much as possible.



The right to information is crucial for ensuring public awareness and trust, fighting misinformation, ensuring accountability as well as developing and monitoring implementation of public policies aimed at solving the crisis



## Safe-guarding Kenyans' data amidst a pandemic

Compiled by Ekai Nabenyio

Contact tracing, as a public health management process of identifying persons (including healthcare workers) who have had contact with individuals with probable or confirmed COVID-19 infection, has been applied in Kenya, as in other countries. Contact tracing is meant to identify potential secondary cases that may arise from a primary COVID-19 case. This intervention has helped avoid further onward transmission by victims. The implementation of contact tracing in Kenya by the Ministry of Health, in coordination with law enforcement, has not been without controversy and has raised various human rights concerns. Important considerations include the effectiveness of contact tracing and the concomitant impact on privacy and human rights. The shortcomings of contact tracing go beyond privacy considerations and potentially infringe on other human rights. While the various accounts as narrated by the respondents are true, the names that have been used in this case study have been deliberately modified to hide the true identity of the respondents.

A journalist at The Standard Media Group received reports from Wanjiru Kemboi whose phone calls and other communications were believed to be intercepted by government surveillance agencies. It was also apparent that the affected individuals did not understand their digital rights. Wanjiru who had been subjected to the 14-day mandatory quarantine period contacted the journalist as she had a strong suspicion that her mobile phones were tapped, although she seemed to not be concerned about it. Wanjiru had an experience in which a National Intelligence Service official contacted her, as a patient that was supposed to be on self-quarantine, warning Wanjiru against going to the market and mingling with others on a day when she actually attempted to go to the market. Wanjiru Kemboi complied with the order and retreated back to quarantine. This was a clear testament that the patient was being monitored by the National Intelligence Service in liaison with the Health Surveillance agencies. This meant that the COVID-19 patient lived in constant fear while in private confinement and did not have an assurance about the protection of their privacy. It was also not clear what the extent of the penetration of the surveillance by the National Intelligence Service, and the Health Surveillance, was.

This clearly violated the individual's right to privacy, even in the face of the COVID-19 pandemic, as guaranteed in the Bill of Rights of the Constitution of Kenya, 2010. This revelation raises questions as to how the COVID-19 patient's data is used and how long it should be stored on national security databases. The concern here is the possibility of surveillance by the State, particularly should data use and storage not be legally safeguarded. Individuals' right to privacy can be affected by digital data collection and processing. In developing solutions to address crises, State institutions and regulators should do their utmost to balance the right to privacy and the right to information when there is a potential conflict between them. Numerous other cases were reported, especially after the journalist penned an article to report cases of increased tapping of phone calls by State agencies.

In conclusion, injurious contact tracing that violates human rights breeds suspicions between the State and the citizenry. To right the wrongs that have characterized contact tracing in Kenya, it is recommended that there is an urgent need for Health Surveillance authorities and officers of the National Intelligence Service to comply with the provisions of the Data Protection Act, 2019, as far as the protection of citizen's private data is concerned. The State should take appropriate measures to safeguard data and to regulate who has access to the same.

The Government of Kenya introduced the mSafiri App, a brain-child of a collaboration between Kenya's Ministry of Health and the Ministry of Transport, in containing the spread of the virus. The app was designed to provide critical data that would help trace back the movements of infected or suspected COVID-19 cases. This Digital Health Surveillance tool necessitated the need for the government to be transparent on how the data collected was used but the lack of guiding principles, as far as contact tracing is concerned, was a point of concern raised. There were concerns by particular patients that the Government of Kenya was not able to manage these technologies and therefore contracted third parties-technology companies. As a result, this has presented an opportunity for abuse of health surveillance data as there are no known Data Sharing Agreements with such third parties. This is critical as it is feared that intra-government use of data in Kenya may be mostly utilised for security reasons; there is a need to safeguard against this.



To right the wrongs that have characterized contact tracing in Kenya, it is recommended that there is an urgent need for Health Surveillance authorities and officers of the National Intelligence Service to comply with the provisions of the Data Protection Act, 2019, as far as the protection of citizen's private data is concerned.





## TogoSafe application's data grab

Compiled by Seyram Adiakpo

The TogoSafe application was conceived by the Togolese Ministry of Posts and Digital Economy in the context of COVID-19, to track and follow travelers in-country. The app was compulsory for all travellers arriving in Togo. Besides the compulsory downloading of the application, the traveler is required to sign up to the corresponding government website. However, due to several factors, the application presents issues relating to digital rights and freedoms' violations.

On the question of data, the general conditions for utilization remain silent. It is only said that the application is designed to "monitor the user's movements but not expose their private life". This brief affirmation is made with no clarification on the way the user's private life will be protected and the users' data will be kept from any other use than that mentioned above.

Furthermore, the user has no idea of the exact data collected. The user is only ordered to keep the Bluetooth and GPS services on their devices activated. The user is forced to agree to share their data without knowing which data is being shared, otherwise, they are placed in quarantine within the monitoring structures set up by the State at their own expense.

The government site reads, "People in lockdown must respect the strict rules while keeping the TOGOSafe application activated while awaiting results of the COVID-19 PCR test." They have to abide by such unexpected control by security agents and health workers at their place of lockdown.

In addition, the application is available on app platforms such as Google Play, App Store and the App Gallery. On the app's website, it notes that data is not shared with third parties without the third parties being defined. "The state now voluntarily or forcefully offers personal data to these companies," regrets Anoumou (name changed), a Togolese citizen residing in the United States, whom when passing through Togo was forced to download the app before entering the country.

Four other people contacted as part of the study said they had no choice but to accept. Users are not informed about whether they can access the data collected, oppose it or have it modified or deleted unless they go to the website of the application, which not everyone has the instinct to do.

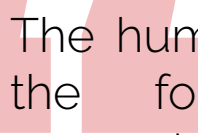
Users who download the application do not have enough information on the general conditions of use.

In Togo, Law No. 2019-14 of October 29 2019 details the principles relating to the protection of personal data. Under this law, provision is made for the creation of a Personal Data Protection Authority (IPDCP). It also states the existence of the Independent Administrative Authority (AAI) which is responsible for ensuring that the processing of personal data is carried out in accordance with the provisions set out in the law. If the legal framework that protects personal data is absent, it becomes difficult for the traveller to have an open dialogue, resulting in difficulties in having their data modified or erased. They will have to engage the developers of the application, which might result in a lack of transparency.

On the issue of transparency, the management of the TogoSafe app is not open-sourced even though open data would give civil society and academia the opportunity to assess the application. A human rights-based approach has not been taken into account in the management of the TogoSafe application. When it comes to digital rights, the human rights-based approach mainly concerns the legal framework put in place by the State, but also its attitude towards citizens. The human rights-based approach includes the following principles: participation, accountability, non-discrimination and equality, empowerment and legality.

In addition, the application challenges medical confidentiality. The medical data of people who test positive for COVID-19 is shared with the entity that manages the application. This sensitive data is made available to the entity. The purpose of the application must be clearly defined.

The State should make users more aware of the risks of using the application without having to find them on their own. Users should be free to opt out of using an application such as TogoSafe. In addition, the application must be brought into compliance with Law No. 2019-14 on the protection of personal data. All technical choices should be documented and explained by the responsible parties. The technical operation of the application should be completely transparent so that users feel responsible for their choice of whether or not to use the application. Finally, the application protocol and its implementation should be documented, public, and independently audited.



The human rights-based approach includes the following principles: participation, accountability, non-discrimination and equality, empowerment and legality.



# The looming threat to data privacy for Nigerians in a pandemic

Compiled by Khadijah El-USman

Nigeria recorded its first COVID-19 case in February 2020 and like many other countries, had to scramble to put resources together to tackle the ensuing effects. And with unprecedented times came unprecedented measures. Governments had to rapidly identify and ensure care for cases, trace and quarantine their contacts and monitor disease trends. Countries like Belgium, Malaysia and Singapore developed web applications and used mobile devices to keep track of their citizens.

Nigeria, on the other hand, has a controversial history with health surveillance with little to no regard for the rights to personal privacy. This was evident from the Governors' Forum trying to use mobile companies like MTN to trace movements, to applications like Stay-SafeNG being developed for contact tracing for COVID-19.

For the average Nigerian affected by COVID-19, their experiences with contact tracing and health surveillance were small scale but helped to give a bigger picture of the problem at hand. For Dr Ade (name changed), after he and a few of his colleagues had come down with COVID-19 like symptoms and eventually tested positive, the hospital undertook contact tracing for him and his colleagues. He described the procedure as "making venn diagrams of clusters of patients we had all seen" and eventually found that all the doctors in question had seen the same patient.

The hospital had its own COVID-19 unit reporting back to the Nigeria Centre for Disease Control (NCDC) who did the contact tracing. Ade noted, "My hospital has the privilege of having all patient information digitized so it was very easy to get contact information of the patients involved," meaning different organizations and the COVID-19 unit had access to patient information without their consent. He alluded further that from his knowledge of epidemiology, "when dealing with a highly infectious disease, you can access patient information pertinent to that issue, meaning address and phone number."

With that in mind, is it questionable why in Lagos State, the Nigerian Institute of Medical Research developed a seven-page Google form to be filled by all those who required testing for COVID-19 at the peak of the pandemic. The form required various details, including office address and next of kin. Eventually, if the person tested was positive then the contacts were traced. There were COVID-19 centers in each local government area with health workers equipped with mobile devices ready to assist those who did not have access to digital tools, although most of these workers were not trained on the principle of confidentiality.

The data of people who tested negative or were never infected, including that of their next of kin, were uploaded into a third party database, leaving the question of who stores this data, and how long it will be kept in light of the lack of data protection laws, unanswered.

On the other hand, Dayo, another respondent in Abuja, had a different experience when the NCDC came to test him and his colleagues. There had been an outbreak in his office and everyone had to get tested. Dayo noted that the process was not very digitized; "it was a very manual process." The NCDC representatives came with numerous forms that posed various questions and to Dayo, "many of the questions did not seem necessary but they came with a counselor to seek your consent. Even though it felt like an invasion of privacy, I could see the point". To Dayo, it did not seem like any of the information being taken was going to be inputted into a system or database. Dayo shared that if this information were to indeed be inputted into a system, he would be worried about his privacy and the stigma that could come with certain information. Dayo went further to report that this fear had many of his colleagues inputting fake information on the NCDC forms. Should there be any abuse of privilege in the near future, Nigeria's lack of comprehensive data protection laws leaves Dayo and others like him vulnerable.

Public health data is usually personally identifiable and sensitive, often revealing details about a person's lifestyle, behaviors, and health. With not only the government involved, but also third-party actors including application creators and pandemic volunteers being privy to the data of Nigerians, there needs to be a call for accountability. There is a need to address the right to personal privacy, especially related to public health issues, and utilising a human rights approach in creating policies that have the capacity to not infringe on people's rights.

“There is a need to address the right to personal privacy, especially related to public health issues, and utilising a human rights approach in creating policies that have the capacity to not infringe on people's rights.”



# COVID-19: Between personal data breaches and disinformation in Cameroon

Compiled by Rigobert Kenmogne

At the beginning of 2020, Bernard (name changed), 60 years old, went to Europe as usual. But this visit would not be like the others. His stay in April 2020 coincides with the start of the Coronavirus lockdowns. Originally from the western region of Cameroon, Bernard plans his return to Cameroon to avoid the worst. Once in the country, via Douala International Airport, Bernard must undergo tests as indicated in the health protocol in times of crisis.

Several other passengers like Bernard are waiting for their tests to be carried out with long waits as health services are saturated and are still adapting. Bernard is a well-known personality in the country. Given his age, he must be attended to as a high risk patient as is the case with other elderly passengers.

Bernard tested positive for COVID-19 and went into quarantine. During quarantine, he did not survive and his death left his friends and colleagues in shock. He was an emblematic figure of his community. Despite receiving assistance from healthcare workers, as well as friends and family, Bernard died from COVID-19. During his quarantine, several family members and friends came into contact with him, most of whom did not have a real knowledge of the dangers of the virus yet.


Bernard's funeral was organized in strict compliance with barrier measures away from his native village. A few days later, after Bernard's funeral, friends and relatives became aware of a publication on social media brandishing his COVID-19-related personal data. The news is received with doubt given the denial amongst many Cameroonians of the virus' existence. The announcement with the photo of Bernard a few days after his funeral created a panic in the community. There are mixed sentiments from some refusing to be tested to others seeking home remedies to treat the virus. There is also anger following the publishing of the deceased's personal information.



Other COVID-19 cases that have been disclosed on social media have also created shock in the community as noted through the work carried out by Merveilles du Monde (1) through the International Foundation for Development, Education, Entrepreneurship and Environmental Protection (FIDEPE) in Cameroon. A team member says: "The second case for me was even more stigmatizing. After Bernard's death, a false announcement spread about the contamination of his private secretary. This situation plunged the whole community into turmoil a second time, with the fear for everyone to approach a member of the different families. It was later that the private secretary of the deceased arrived in the village a few weeks later and in good health, very angry, after having published a post in advance on Facebook to express his dissatisfaction to all those who disseminated this false information of a positive test for COVID-19 with his photo."

The messages of support enabled Bernard's private secretary to organize awareness-raising campaigns alongside Merveilles du Monde. "He organized an anti-COVID-19 awareness and response campaign in his community," indicates a member of Merveilles du Monde. For the third case, the member adds that, "This was a man who had health problems for a long time before the COVID-19 crisis. After his death, images were broadcast on social networks announcing a subsequent death from COVID-19 when his test was negative."

In each case, Merveilles du Monde provided psychological and social assistance as part of the campaign. To limit such violations, in similar crises, Merveilles du Monde recommends "setting up wider platforms for discussion and awareness of the risks of personal data exposure in times of crisis". In general, awareness training on the consequences of these violations during the crisis is necessary.



Merveilles du Monde recommends "setting up wider platforms for discussion and awareness of the risks of personal data exposure in times of crisis". In general, awareness training on the consequences of these violations during the crisis is necessary.

1. <https://www.merveillesdumonde.org/page/848934-qui-sommes-nous>



## COVID-19 Case No.15: A Zimbabwean victim of misinformation

Compiled by Thobekile Matimbe and Everson Mushava

A Bulawayo lady who tested positive for COVID-19 at the inception of the recording of cases in Zimbabwe was subjected to brutal attacks online. This followed a release by the government, in the Chronicle newspaper, that the patient – Case No. 15 – was violating COVID-19 regulation by escaping from quarantine, and posing a health risk to the community. Unfortunately, as a result of this, Case No.15 got to hear the news of her status through social media, leaving her victimised. The system of disclosure of information was flawed and had no regard for the protection of personal information of patients. For purposes of preserving the identity of Case No. 15, this case study refers to her as X.

On April 16 2020, the Chronicle newspaper ran an article on X expressing concern that she was Case No. 15 yet gallivanting across the city of Bulawayo, spreading COVID-19 in blatant disregard for isolation as required of positive patients. The headline was titled, "Beware of this patient! COVID-19 positive woman gallivants around town." The article gave an exposition of X disclosing that Case No. 15 was a health worker breaching COVID-19 guidelines after a positive test result. It portrayed her as a reckless individual.

Information gathered revealed that X was screened for COVID-19 on April 12, 2020, using a thermometer and turned out to have a high temperature. She was then tested for COVID-19 by a Rapid Response Team which advised her to wait for 48 hours to access her results. On the night of April 14 2020, X then received messages on her cell-phone from colleagues who were checking if she was alright. She discovered a COVID-19 update report released by the government which was describing her as Case No. 15 amongst the new messages on her phone.

"I checked my inbox and came across the daily update from the Ministry of Health and Child Care and immediately realised that Case No. 15 was referring to me as had a number of my colleagues. I resolved to await official communication from the Rapid Response Team who only came through

1. See CITE <https://cite.org.zw/COVID-19-case-number-15-speaks-out/> (accessed on 10 March 2021)

to my residence on Tuesday, the 15th, at 1430hrs.(1)”

That was her first encounter with her results. The government, through the Rapid Response Task Force, failed to reveal X’s results to her before disclosing them publicly. Her colleagues were able to also gather from the description in the report that X was positive of COVID-19. X was appalled by having to find out of her COVID-19 status through social media.

As if this were not enough, X was even more shocked when the Chronicle released the article on April 16, 2020.

“[Imagine] my shock when in the wee hours of the morning on Thursday the 16th of April, 2020, I received a link to the publication by the Chronicle accusing Case Number 15 of recklessly endangering the lives of residents by defying self-isolation. Social media has since been awash with the news which begs me to ask whether there is another Case Number 15 or is this just a case of unethical journalism,(2)” expressed X.

The newspaper article in the Chronicle is no longer accessible at the time of writing this story. Through the article, the government peddled false news about X. The false news found its way on various online platforms such as WhatsApp and Facebook. The government later clarified that X was not guilty of the allegations made against her through an article in the Chronicle on April 18, 2020, titled “COVID-19 defaulting patient taken to Thorngrove.(3)” This new version in the Chronicle disclosed that there was a mix up as Case No. 15 was not the individual who had breached COVID-19 isolation procedures as revealed by health officials.

There is a need for the government to ensure that safeguards are in place for adequate privacy and personal data protections.(4)

“...Unfortunately, as a result of this, Case No.15 got to hear the news of her status through social media, leaving her victimised. The system of disclosure of information was flawed and had no regard for the protection of personal information of patients.

2. n 1 above.

3. <https://www.chronicle.co.zw/COVID-19-defaulting-patient-taken-to-thorngrove/> (accessed on 12 March 2021).

4. See UN ‘COVID-19 and Human Rights We are all in this together’ page 22.



# Protecting the privacy of Zimbabwean COVID-19 patients

Compiled by Thobekile Matimbe and Everson Mushava

Zimbabwe recorded its first COVID-19 case on March 21 2020 amidst an unprepared healthcare system. Slowly, the numbers of COVID-19 recorded cases started growing. Amidst these cases was the misfortune that befell Saul Sakudya, a Harare businessman.

Sakudya was the third recorded case of COVID-19 since the outbreak started in March 2020 in Zimbabwe.

According to Sakudya, he presented the tell-tale symptoms of coughing and feeling dizzy after his return from a trip to Dubai on March 19 2020. He consulted with medical practitioners but his situation did not improve. Sakudya resolved to visit Wilkins Infectious Hospital (Wilkins) which was the only designated hospital handling cases of COVID-19 at the time. His 21-year-old son drove him to Wilkins and Sakudya was tested for COVID-19 but did not immediately access his test results.

"I was told that my results would come out in five hours and if they didn't, it would mean that I had tested negative," said Sakudya.

He went home to wait for his results, anxiously. It was only on the third day that Sakudya received a call that he had tested positive. According to Everson Mashava, a journalist who conducted the interview with Sakudya, the Ministry of Health permanent secretary, Ms. Agnes Mahomva, confirmed to The Standard newspaper at the time that COVID-19 test results were indeed meant to be delivered within five or seven hours.

The delay in receiving an update on his results caused much anxiety. The Ministry of Health officials then took samples for testing of Sakudya's wife and son as they were his caregivers, as well as his 10-year-old daughter. This was part of the contact tracing response to COVID-19 by the taskforce handling the disease.

In the meantime, Sakudya was placed in quarantine at Beatrice Infectious Diseases Hospital in Harare. He suffered from stigmatisation at the hospital as COVID-19 was a new and terrifying phenomenon to the medical personnel at the hospital. The medical personnel at the time had no adequate personal protective equipment and as such were fearing for their lives. In this chaos, Sakudya opted to go back home to quarantine in a more conducive environment for his recovery.

What was even more disconcerting was that before his family received their test results, social media users had received information that two of his family members had tested positive of COVID-19. Apparently, the government published the new cases before revealing the results to the patients in violation of their right to accessing information.

"It was saddening that results came after announcements were made and were already circulating on social media. That is not good," expressed Sakudya in a state of dismay. "We received several calls from relatives, friends and neighbours who told us that social media was awash with news that three family members have tested positive to the virus. This was before the Ministry of Health officials came with the results. It was very traumatizing for my wife and son to learn of their health status on social media." True to the results circulating online, Sakudya's wife and son tested positive, while their 10-year-old daughter tested negative.

Sakudya's wife mentioned that she was a victim of social media bullying. "It was a painful experience. Firstly, I was described as a small house, a home wrecker, and then, my COVID-19 results going viral without me knowing them," she said.

Sakudya's 21 year old son also expressed concern at the "apparent disregard for confidentiality of the family's health status." He mentioned that his family suffered stigmatisation as a result of the positive results.

The Sakudya family experienced trauma both through the delayed disclosure of COVID-19 results and the failure to exercise due caution in the release of the results in March 2020. There were clearly no effective data protection measures in place to ensure a level of care taken in informing the patients of their results. Such measures would, for example, provide for the publication of updates of new COVID-19 cases after the individuals concerned were notified of their results. Furthermore, there was a need to put measures in place to protect the privacy of the patients who tested positive for COVID-19.



Furthermore, there was a need to put measures in place to protect the privacy of the patients who tested positive for COVID-19.





Paradigm Initiative  
HQ: 374 Borno Way, Yaba, Lagos - Nigeria.