Webinar Report: Regulating the Migration of Health Data in Africa

This event was the first of an international webinar series aimed at networking, fact-finding and bringing together different stakeholders in data handling, data management and protection of mHealth applications, particularly within the African context. The research project leading to this webinar was enabled by a researcher from the WELLCOME Trust granted to the host Dr Sharifah Sekalala of the University of Warwick. Collaborating institutions on this grant are the University of Nairobi (Kenya) and the University of the Witwatersrand (South Africa). This online event took place on the 14th of April 2021 from 11:00hrs to 14:00hrs EAT and was moderated by Dr Ben Mkalama.

There were participants from Kenya, Uganda, South Africa, United States and the United Kingdom.

Key discussions fell into the following categories:

The Keynote as addressed by the Data Commissioner in Kenya was on *Data Protection in mHealth Applications in the Context of an African Country*

This was then followed by the following panel discussions and topics:

1. Transnational Regulation of health Data Migration – Today and Beyond
2. Ethics and regulatory issues related to mHealth Applications
3. Cybersecurity and its implications on Health Data Management
4. The Challenges around data use and storage in mHealth Applications
5. The generation and ownership of data from mHealth Applications.
6. mHealth Innovations Scenarios

Key participants:

- Immaculate Kassait, Data Commissioner of Kenya
- Dr Sharifah Sekalala, Associate Professor of Law, the University of Warwick (United Kingdom
- Professor Pamela Andanda, University of the Witwatersrand, Johannesburg (South Africa)
- Prof. Bitange Ndemo, Professor of Entrepreneurship, University of Nairobi (Kenya)

In addition to the key participants, the following were also active discussants in the event:

- Ms Siobhan Green, Digital and Data Governance and Transformation Portfolio Manager, IMC Worldwide
- Mr Paul Mbaka, Head of mHealth, Uganda.
- Dr Harriet Etheredge, Ethics and Regulatory, Donald Gordon medical centre
- Mr Evans Kahuthu, Data Security Expert
- Mr Mugambi Laibuta, Mediator & Policy Legislative Drafting Professional
- Mr Kwame Rugunda CEO, Savannah
- Dr Shiko Gitau, CEO, Qhala
- Mr Al Kags, CEO, The Open Institute

Opening session:

Data, as we know it, has become an extremely contentious and vastly disputed issue.

The opening session was addressed by Dr Sharifah, who began the discussion by mentioning that in 2018, 'The Economist' held that data was becoming more valuable than oil. The COVID-19 pandemic that has since plagued the world has brought to the fore some critical concerns regarding data collection, storage and management, among others.

Therefore, this event came at an opportune time when Africa should be seeking answers to these concerns:

- How does data move?
- Who owns it?
- How should it be used?
- Who should have control over it?
- Who should have access to the data, and how long should such access be granted?
- Who should govern the management of the data?
- Who should have oversight over that governance?
- Under what conditions should data be collected?
- What do the users think about their data?
- How has regulation changed? Whereby we think about it within the widest frameworks, e.g., what has happened to traditional regulators such as the medical boards; do they regulate the space at all anymore?

The webinar's deliberation focused on data and considered how mhealth applications work, who are the people involved in creating them, who uses them, and how Africa could ensure Sustainable Development Goals (SDGs) in achieving better health outcomes moving forward.

KEYNOTE: Data protection in mHealth Applications in the context of an African country

Data Protection

The Keynote was addressed by Ms Immaculate Kassait, who is the first and current Data Protection Commissioner (DPC) in Kenya under Kenya's Data Protection Act (2019) (DPA). In her introductory address, the DPC acknowledged the importance of the webinar as it came at a time when regulations on data protection aimed at aiding in the operationalising of the Data Protection Act had been released to the public for review and feedback.

The need to protect and safeguard personal data is highly critical, especially when there are numerous advancements in technology and business exchange. Likewise, the *right to privacy* is a fundamental human right under the Universal Declaration of Human Rights (UDHR) and, as such, is espoused in constitutions globally.

As established under the DPA, the Data Commissioner's office came into force on 16th November 2020. So far, this office has embarked on operationalising the DPA with a focus on four priority areas:

- Establishment of internal structures.
- Development of operational frameworks, including regulations.
- Creating awareness.
- Involving stakeholders as well as international collaborators

Draft Regulations under the Data Protection Act of Kenya

Accordingly, a task force that had been appointed and gazetted in January had come up with the following draft regulations:

- Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021[1]: This regulation sets out the procedure that will be adopted by the data commissioner in registering data controllers and processors as per the act.

- Data Protection (Compliance and Enforcement) Regulations, 2021[2]: This regulation outlines the enforcement provisions and the exemptions under the DPA
- Data Protection (General Regulations), 2021[3]: talks about the data subject's rights, duties, and obligations.

mHealth had over the past decade, become an increasingly important part of mobile communication technology and an integral part of the healthcare provision process. In this regard, it was noted that great strides had been made where mHealth is concerned.

As with any other innovations, there is a rising concern regarding the safety of the mHealth applications on matters such as the safeguard against disclosure of sensitive personal information of patients to unauthorised parties or accidental leakages to the public. Thus, concerns regarding data ownership, data storage, localisation and transfer, and data user arise. Bearing in mind that there is always the additional concern that consumers of such innovations are often uneducated on their Data Protection Rights and how their application collection share personal information with third parties in Sub-Sahara Africa and globally. For this reason, Kenya's DPA not only has its provisions anchored on international best practices but also has into consideration the practicalities of each provision in a Kenyan context and with the data subject at the centre.

Taking into account the innovation strides in Kenya, for issues such as mHealth, the Act provides:

1. The absolute requirement for all entities to ensure they have data privacy by default or by design that caters for the technical and organisational safeguards and protection of personal data with increased responsibility on persons collecting sensitive personal data such as health or biometric data.
2. Give ownership and control to data subjects of their data. In this regard, data subjects must give informed consent to collecting their personal data, giving consent to sharing and transferring their personal data, including cross-border transfer and the exception to the retention of processing of their data.
3. For enforcement and penalties of persons and entities who breach the right over data subjects and(or) fail to take necessary precautions as envisaged under the Act to safeguard personal data and uphold the subject's rights.

The DPC further noted that "If the pandemic has taught us anything, it is that there is now more than ever an increased need for collaboration between public

and private sector across borders. The pandemic has necessitated the need for an open exchange of information to tackle health emergencies."

In conclusion, the DPC established that cross-border transfer of data in technological and organisational data and in the presence of consent, where sensitive data is concerned, is permissible under the Kenyan DPA.

Questions raised to the keynote speaker were:

- To what extent was the account taken on trans-border issues and trans-national data movement when coming up with the framework?
- Whether the regulation provided for issues beyond traditional patient data such as emerging biotechnology, for instance, genomics and biomarkers?

The DPC confirmed that cross-border issues were taken into account, ensuring that there were adequate mechanisms in Kenya where the cross-border transfer is concerned.
Matters cross-border of data remain one of the finely contested issues.
Concerning the second question, it was noted that the regulations are general but have provided for limitations, especially where primary data healthcare is concerned.

Panel Discussions:
Session 1: Transnational Regulation of Health data migration - Today and Beyond

This session was moderated by Professor Pamela Andanda, a Professor of Law at the University of Witwatersrand, South Africa. Other panellists in this session were:

- Mr Paul Mbaka, Head of mHealth, Uganda
- Ms Siobhan Green, Digital and Data Governance and Transformation Portfolio Manager, IMC Worldwide

Professor Pamela facilitated the discussion, inviting panellists to reflect on the following concerns:

- *How is mHealth being used in African countries?*
- *How can health apps help African Countries to achieve SDGs?*
- *What are the challenges of using data from health apps?*

The main points that emerged during the discussions are outlined below.

Public trust as a critical component in data handling and management in general:

On the issue of how data can be used for decision-making, it was found that across different African countries, technological tools, especially for mobile service delivery, had proven effective at better healthcare service delivery, as well as collecting valuable data that would go a long way in providing spot-on and responsive support to communities.

Data Sensitivity and privacy

Sensitivity is relative in that what one person may consider sensitive may not necessarily be considered so by another person. Therefore, understanding and putting that human-centred piece of information at the forefront would be necessary for ensuring trust among individuals and entities.

A case in point mentioned was the marginalised communities such as HIV/AIDS patients, who tend to be slow to trust and rapid to distrust. Such communities value privacy to the extent that many times they implore behavioural strategies to protect their privacy. Such strategies would involve using different names, different identities, using proxies, or having somebody else go and collect their medications or act on their behalf. They, in some instances, would also travel to different health facilities. This then interferes with data management.

Therefore, in trying to promote health from a digital perspective, privacy and protection are of utmost importance bearing in mind that people may not be aware of some of the risks to their data. However, as soon as they know about them, it becomes a significant part of their decision-making.

One of the reasons why cross border data sharing is essential is that people do not necessarily see borders when seeking healthcare. It was found that in some parts of the border between Kenya and Tanzania, women were seeking prenatal care in Kenya because they thought it was of higher quality and there were lower-cost implications for them, but they would then give birth in Tanzania because they got the birth certificates on site right after the birth. In such a case, merely looking at the aggregate data, it would be presumed that Kenya has got more outstanding prenatal care but terrible birth and health facility numbers. And then the vice versa would be true in Tanzania, while this is not entirely the case. Therefore, if a population is not being looked at holistically, how would it be possible to understand what is happening and have appropriate interventions to support those aspects?

Poor Infrastructure

Uganda faces infrastructural and record-keeping challenges in their attempt to deliver health services. Due to these challenges, Uganda deployed several digital health tools used in areas such as mobile screening points. This is in addition to client-facing tools such as remote monitoring tools for patients with some non-communicable diseases that can quickly provide them with feedback on some of their vital signs.

Some of the tools deployed are SMS based and act as good reminders, mainly because they have a broad reach. They also have limited technological constraints faced by digital tools that rely on the internet. Uganda also has vibrant community surveillance mechanisms that allow members of the public to generally report on any suspicious either deaths or diseases that they observe.

The risk of technology and innovation outdating policies

Recognisably, it is common for innovation to outpace regulations. Therefore many times, such innovations first come in place before figuring out where the pitfalls and the places that need tightening, by way of regulation are. Moreover, even the experts in the area may not be those participating in policy formulation, thus posing another challenge in Uganda, for instance, with regard to policy formulation around technology and data.

Additionally, there is a risk posed by the speed of progression in the general area of digital health production. The explosion of Artificial Intelligence (AI) and Machine Learning (ML) can render regulations that seem relevant today to be obsolete within any short-given period. Thus it poses a challenge to policymakers to craft laws with a precise forecast of possible uses of data collected from mHealth apps.

Uganda passed its Data Privacy and Data Protection Act in 2019, and it is in its formative stage of implementation. Just like in Kenya, the Act has general provisions. However, it is expected that with regulations and possible policy guidelines, some areas might be tightened.

Cross-border data transfer

Uganda faces a challenge in that its health sector does not receive sufficient help from the government. This causes an over-reliance on donors who, in some instances, bring onboard conditions such as data sharing. Availability of resources, including manpower and financial resources, limits the scope of data protection and monitoring.

Data Record-keeping

It was noted that digital record-keeping also posed a significant threat since having the patient's data in a single location made it easily accessible even to

unauthorised parties. At the same time, trusting that a patient would keep their records safe at home is impractical. A possible solution would then be digital health cards that the patients can carry around containing their details. The cost factor of implementing these cards was found to be limiting on a larger scale in Uganda.

A question raised in this session was:

- What can Africa do with regard to the donor situation?

It was suggested that African states consider better negotiations with the donors bearing in mind that many of these donors, angel or venture investors, may have a vested interest in the data collected.

Session 2: Ethics and regulatory issues related to mHealth Applications

The sole speaker in this session was Dr Harriet Etheredge, medical ethics computation specialist based in, in South Africa.

In her discussion on the ethics and regulatory issues related to mHealth applications, Dr Harriet focused on clinical management and data management aspects.

On the data management aspects, mHealth apps have since created a new ethics framework that has unique challenges because an mHealth app has two distinct applications:

1. **Clinical management tool:** which aids in getting points of care management out there and how valuable mHealth apps can be in helping healthcare reach people who have not had easy healthcare access before.
2. **Data Generation:** mHealth apps also, generate a lot of data by virtue of their structure.

These create a new clinical modality, whereby it is not just a doctor-patient relationship; instead, it involves mHealth business issues such as data storage and data generation. Thus, raising several ethical and legal issues that relate to regulation. Data generation, data transfer, jurisdiction, data protection, and data storage on the business side come to the concern. On the ethical side, we have concerns for confidentiality, informed consent, accountability, future use, and transparency.

Lack of clear mHealth regulations in a South African context:

South Africa has a traditional clinical, regulatory framework made up of various pieces of legislation. They include the Constitution of the Republic of South Africa (1995), National Health Act No. 61 of 2003, Health Professions

Amendment Act No. 29 of 2007 and the Allied Health Professions Act No. 63 of 1982(as amended).

It also has ethical conduct guidelines and professional councils that regulate the conduct of healthcare providers, accreditation and credentialing. In some cases, there are clinical risk assessments, clinical ethics committees and professional societies. All of these people or institutions have a role in regulating South Africa's clinical practice. This then becomes relevant to mHealth since it, too, has a clinical aspect.

However, mHealth as an individual entity lacks clear-cut regulations in South Africa and many other African countries. Therefore, in South Africa, there are inexhaustive legislations that can apply to mHealth in specific ways, but none of which relate to mHealth directly, leaving regulators with the task of picking out the relevant aspects of these pieces of legislations. These include;

- Protection of Personal Information Act No. 4 of 203
- Films and Publications Amendment Act No. 11 of 2019
- Employment Equity Act No. 4 of 2013
- Protection from Harassment Act No. 17 of 2011
- Regulation of Interception of Communications and Provisions of Communication-Related Information Act No. 70 of 2002
- Electronic Communications and Transactions Act No. 25 of 2002
- Promotion of Equality and Prevention of Unfair Discrimination Act No. 4 of 2000
- Labour Relations Act No. 194 of 1993
- Cybercrimes Bill (still in Parliament)

Collaboration in a cross-border context

With the capacity for data generation Africans use the data collected for research and development at a continental and global landscape. This will work towards bridging the historic north-south divide in issues such as where we find drugs developed. However, they do not have representation from Africa, publication recognition for work done in Africa, and so on.

Data Generation through mHealth

mHealth apps generate vast volumes of data that can inform other applications such as research and development. Sharing this data is essential for:

- Open Science
- African representation in large datasets

- Bridging the historic “North-south divides in research
- Publication
- Furthering knowledge generation in the public interest

Therefore, the benefits of data sharing need to be carefully balanced against risks of group harms and possible stigmatisation.

Regulation in a research context

South Africa has a legally mandated Material Transfer Agreement, which also extends to identifiable data. This has to be agreed upon at a legal and ethical level. Additionally, export permits are required to send materials such as tissues or biosamples internationally.

Regulation of data in a research context is also starting to look at cloud storage and security, but this is another complex aspect because these cloud storage platforms keep changing and new ones emerge and they change their terms and conditions, which further poses regulation challenges.

All these is in addition to South Africa’s traditional pieces of legislation.

Protection of Personal Information Act No. 4 of 2013 (POPIA)

This Act is set to come into force on 1st July 2021 in South Africa. It has both clinical and research applications and implications. It emphasises people's right to privacy through several different safeguards.

About cross border data sharing, POPIA notes: In principle, responsible parties must ensure that the country with which personal information is being shared or transferred to has a high level of data protection as offered under POPIA. Thus, transfer agreements must be in binding contractual form.

Where no adequate protection is in place, additional safeguards must be provided by the data exporters and importers to guarantee such protection or suspend transfers of data to the particular country.

Session 3: Cybersecurity and its implications on Health Data Management

The sole speaker in this session was Mr Evans Kahuthu, a Data Security Expert.

Globally, data **is very enticing, especially for criminals and for anybody who wants to get into cybercrime.** In as far as healthcare is concerned, there are two sources of risks, internal and external.

The internal risk, which is just as high as the external, involves doctors, nurses, cleaners, et cetera—everybody involved in the healthcare industry and has access and privilege to patient data.

The problem with health data

Health data possesses information of high monetary and intelligence value. Consequently, health data is of a higher value on the dark web. The collection of such sensitive data thus poses a risk to high-risk populations. In Tanzania, for example, children with albinism are hunted for their body parts. This is due to the barbaric belief that their body parts can be used to harness magical powers; hence their value is higher. Collecting such data concerning their health thus becomes a cybersecurity threat.

This is in addition to other targeted patients' data such as the Protected Health Information (PHI), financial information such as credit cards and bank account numbers and so on.

Cyber Threat to Patients

In as far as the patient is concerned, the loss of medical data has become a problem. Losing access to medical records and lifesaving medical devices, such as when a ransomware virus holds such information hostage, deters the ability to care for patients effectively. A case in point is the UK's NHS ransomware attack in 2017[4].

Furthermore, hackers' access to private patient data opens doors for theft of the information. It may also jeopardise or alter, intentionally or not, patient's data, which could lead to severe effects on the patient health and outcomes. For instance, with advancements in medical technology, advanced heart pacers have connectivity from where the pacers relay the data back to the doctors, which is necessary in case of an emergency. Such a heart pacer can be compromised in case of a cyber-attack.

Cyberattacks on electronic health records and other systems also pose a risk to patients' privacy because hackers access PHI and other sensitive information. Also, with such a breach, insurance companies on finding out that patients have pre-existing conditions, may be hesitant to provide health covers for them.

How unauthorised access occurs

People are **rushing to innovate**. Unfortunately, the innovation does not consider the regulations and the technical standards that need to be considered. Thus, mHealth applications are channelled out without proper security in place.

There are also risks with the **Application Programming Interfaces (APIs)** with which developers integrate sensitive information such as healthcare data. This could be in the labs, hospitals or with the medical insurance companies. These

provide easy access to people's data and thus can easily be compromised as well.

Malicious software (Malware) has also become a major risk to cybersecurity over the years. This may exploit a vulnerability in an application or use social engineering techniques to trick the user and install itself on a connected device. The installed malware would then obtain sensitive health information, damage it, alter it, or send it to an untrusted entity.

Lack of ethics among the application developers. There is a growing concern with developers deliberately leaving "backdoor" access to the applications they build, allowing them unauthorised access to the same applications.

Users of mHealth applications also pose a threat to their data security, whereby many of them tend to share the passwords to their devices or applications with others. Also, where they lose their devices, people with the technical know-how can easily unlock the devices and retrieve information if the passwords are not encrypted.

Recommendations for cybersecurity

System and data protection – **Ensure Encryption is implemented.** Knowing that data might be accessed remotely, ensure all access points are encrypted.

Vulnerability Management- Implement Secure System Development Life Cycle (SSDLC). Vulnerability management involves following laid down standards of procedures without skipping a single step. This is very crucial, especially when outsourcing the application development.

Asset Management- Only authorised devices should be granted access to the organisation's data. The authorisation ensures that people only get to see what has been approved by management and what concerns their specific job function. Simultaneously, not every device should be allowed to connect to the corporate or to the healthcare systems.

Compliance – the mHealth app must maintain and protect the confidentiality, integrity and availability of personally identifiable health information in a way that meets regulatory frameworks within the jurisdiction of the data processor.

Built-in ability to clear app data (a data wipe) in case of compromised information from a web download.

Ability to detect and deny apps running on rooted or jailbroken devices. Pirated or compromised devices cannot guarantee security. Technically we should not allow our Mhealth applications to run in these particular devices

simply because we will not be able to guarantee the security of those applications under such devices.

Run checksum on the app's core files to detect if a hacker has tampered with it. This helps us confirm the integrity of both the devices and the application. It also acts as a check for activities as those that have been technically tested and approved by management and by the technical team.

Application Programming Interface (API):

- Use HTTPS back end for all API calls
- Make sure authentication expires after a reasonable amount of time.
- Put API call limits on the server-side - that is, authentication should expire regularly.

A culture of cybersecurity where the staff members view themselves as proactive defenders of patients and their data will have a tremendous impact in mitigating cyber risk to the organisation and patients.

In conclusion, if people become aware of the implications of cybersecurity in healthcare data privacy, this would go a long way in mitigating some of these risks.

Session 4: The Challenges around data use and storage in mHealth Applications

The sole speaker in this session was Mr Mugambi Laibuta, a Mediator & Policy Legislative Drafting Professional.

The Data and the Technology

Data mapping and data inventory - it is essential to know what kind of technology is being developed and what kind of data it is intended to collect, and for what use the data will be. Data collection related to the patient's lifestyle and medical treatments could be relevant in future diagnosis if the need arises. However, this may also prejudice the patient's travel history, occupation, pre-existing conditions et cetera. In addition to requiring information be manually input by the user, some devices also ask for access to the device's calendar, storage, clock, and camera.

The universal principles related to data protection include:

- Lawfulness, Fairness and Transparency
- Purpose limitation
- Data Minimisation
- Accuracy

- Storage limitation
- Security
- Accountability

Lawfulness, Fairness and Transparency

Article 31 of the Constitution of Kenya, 2010 provides for the *right to privacy.* The Data Protection Act of Kenya also aims in upholding lawfulness, fairness and transparency. Unfortunately, Kenya has not yet signed the Africa Union Convention on Cyber Security and Personal Data Protection, 2011, which was drafted to establish a credible framework for cybersecurity in Africa.

Not following the law: While there is some effort among African states in promoting cybersecurity, having a vaguely regulated environment creates loopholes through which developers can work outside the law.

For instance, a company such as Facebook will strictly adhere to the General Data Protection Regulations (GDPR) as stipulated under the EU law. However, in Africa, where we have a disjointed and very shallow application of data protection regulations, the same company will operate flexibly, not affording the same duty of care in Africa as that in the EU.

Not carrying out data protection impact assessment concerning the technology being deployed. Kenya's DPA provides that where there is sensitive data, such as health data, which is high-risk data, a data protection impact assessment must be carried out.

Many people deploying these applications do not want to carry out that data protection impact assessment.

No prior, free and informed consent. A lot of these applications follow **dark patterns**. This involves deploying code or algorithms where it is tough for the individuals, the data subjects, to understand what it does precisely or even opt-in and opt-out mechanisms are pretty hard.

No contractual obligations between controller and processor vs data subject; many data processors and data controllers do not come into contractual obligations in their operations or even in their operation with the data subject.

No public purpose – public health, e.g., COVID-19 Data; TB and HIV surveillance, DHIS2; In some instances, the data harvested does not serve a public purpose and is merely for use in private research or surveillance purposes, which might not be in accordance with many data protection laws. On the issue of transborder sharing of personal data, for example, in West Africa, the West African health organisation created by a statute of ECOWAS states the use of

health data and sharing data between the state members in other regions of Africa.

No obligation to comply with written law-e.g., taxation, investigations, judicial processes. Where there are legitimate reasons for data collection, which is provided for under written law. Such as data related to taxation, investigation and other judicial processes.

Breach of professional code of conduct; this is in relation to who has access to the data, as was earlier discussed. You have not only the medical professionals, but you also have messengers, cleaners, drivers within a health institution who may have access to this sensitive data. Kenya's DPA provides that health data should be handled by people who are bound by a professional code.

No clear information on technology being deployed (explainability v black box) What is this technology? What are you going to use it for, etc. And you find many people really find that to be hard. In the field of AI already, there is a proposal that one must be in a position to explain their technology. What is its purpose? What kind of data will it be collecting? Who is the targeted data subject, and what are the accountability measures? This avoids having technologies created in a black box kind of environment.

Inaccessible technology – low access to the internet and affordability of devices; Most of Africa's population areas still have no access to the internet and affordable devices. This became a challenge, especially with the lockdown due to COVID-19. In Kenya for example, many students were unable to access online learning platforms.

Purpose limitation

For instance, venture capitalists to technology firms will want to access the data collected as a condition to their capital. Also, where collaborating, the state may want to share this data with donors, who may share the data with researchers. This could be dangerous, primarily where the data may be used for surveillance or unsanctioned research in case of conflict.

Accountability

Here, the question arises as to who bears the greatest responsibility in terms of data protection breaches. Is it the data controller or the data processor? Where there are investors, are they also to be held accountable? Creating a registration system that allows for checks and balances on compliance could be a step in the right direction.

Record Keeping

Many institutions have a challenge with proper record-keeping systems.

The EU's GDPR is very strict on keeping a record of processing operations, while in Africa, due to lack of such clear regulation, people deploying this technology do not do that.

Data Minimisation

While there is potential to collect many data on individuals, data processors should aim to collect only the data relevant to what they want to do. For instance, while collecting data for TB patients, it would be irrelevant to collect data about the data subject's operating system or wifi codes.

Accuracy

The challenge is that algorithms or data collection methods are deployed which do not guarantee accurate data. Some technologies have racial bias, especially wearables.

If you feed AI the wrong, the wrong data, because this technology mirrors, what is out there.

So, suppose society is racially biased and you feed the AI a lot of data from a racially biased community. In that case, the decisions that this technology will make will have a racial bias.

Storage

Are you having the data stored in-country or in cloud services, because if you're using cloud services that are external, that is data transfer? In such a case what kind of agreements do you have with the cloud services?

Are these cloud services private and specific, or are they general, do you know which country these cloud services are located? In that jurisdiction does it have proper data protection regulation?

This also brings the debate between **data residency and data localisation.**

Session 5: The generation and ownership of data from mHealth Applications.

This session was moderated by Professor Sharifah Sekalala, an Associate Professor of Law at the localisationf Warwick, United Kingdom. Other panellists in this session were:

- Mr. Kwame Rugunda, CEO, Savannah
- Dr. Shiko Gitau, CEO, Qhala
- Mr Al Kags, CEO, The Open Institute

Professor Sharifah facilitated the discussion, inviting panellists to reflect on the following concerns:

- *What are the benefits and problems of using different types of health apps?*

- *What kind of data do these apps require users to provide and what do health apps users think happens to data?*
- *Who owns the data from health apps and how is it stored and reused?*

Since the health sector is very specialised, it is advantageous to have different apps that target specific interventions. Thus, there are benefits of using different types of health apps. On the flip side, however, using different health apps for different reasons leads to **data fragmentation, making** a lot of the data wasteful, leading to the proliferation of personal identity.

In a case like Africa, where much of the regulation regarding data is still being developed, data collected is owned by those collecting it, which is quite unfortunate. This is unlike the UK, which has a relatively more advanced framework that enables developers to build applications while allowing for the ownership of the data to be standardised. This way, developers can build their applications on the upper layers without affecting or being disturbed by the lower core layers of biometric data, as we see in our environments where these frameworks for regulation are not yet solidly in place.

In reality, in order for mHealth apps to fully function and have full expression, they require personally identifiable data. Moreover, this **personally identifiable data** will give them the ability to impact the people they are reaching out to. However, the core of the problem lies in managing this personally identifiable data, how it is collected, how to store it, et cetera.

It is believed that technologies like blockchain can help by structuring the data better and enabling the data to be actually owned by the individuals.
In extensive research previously done, people were not careful with their personal records, especially when sick. Hence, it becomes a question of balance over **how ethical the medical fraternity is** in storing and managing medical records.
Furthermore, many deaths could be preventable if doctors had easier access to medical records. For example, a diabetic patient involved in a road accident rendering them unable to communicate can receive better treatment if the doctor can directly have access to the patient's medical record in time.
There still exists some scepticism over companies launching mHealth apps such as Safaricom's digital wallet. The opt-in, opt-out issues at a lot of the telecommunication companies remain a major cause for concern. Thus granting such companies access to sensitive personal data such as health-related data yet users have no control over their data usage practices is highly questionable.

Users should be provided with a way to choose how they want their data to be used.

Therefore, we must begin to interrogate what policies and frameworks exist to protect sensitive personal data. At the same time, we have to be driven a lot more by common sense and a lot less by policy think on matters of data protection.

Value of using blockchain in collecting personal data

In this session, how blockchain could help mitigate data collection and sharing or transfer was also deliberated on. It was mentioned that blockchain brings in value since it decentralises digital identities. Also, blockchains are structured in a way that they give the control back to the owner such that anyone who need to access the data has to make it at a design level.

We also need to carefully think through how that data will be managed at the point of contact, whether someone else has that decision-making power as to what of their data they want to share.

Awareness

At all times, people should be aware of the data they are giving away at any given point. Unfortunately, in Africa, many people are not aware of data private.

Data collection for emergency situations

COVID-19 brought out the benefits of data collection that can be of use in emergency situations. In fact, there have been guidelines in this regard even prior to COVID-19 pandemic. These guidelines are provided for by the World Health Organisation (WHO) and have been there for a long time.

Questions raised in this session were:

- When do we know that an emergency has ended?
- How do we find the right balance between data regulations, ethics, and the actual benefits of accessing and opening data in the context of emerging tech?

In response to the questions raised, it was suggested that there should be policies in place that safeguard people's rights by '**mopping after innovation'.** This will necessitate data processors to clear their databases after the use of the technology has passed. For instance personal data collected in relation to COVID-19, such as due to contract tracing should be destroyed after the

pandemic and there's no longer reason to maintain such data other than what was initially collected for.

There has to be some kind of agreement around multiple governments and even within local governments to make sure that people's rights are protected.

Session 6: mHealth Innovations Scenarios

This session had a single discussant, Professor Bitange Ndemo, a Professor of Entrepreneurship at the University of Nairobi, Kenya.

The uptake of mHealth in Africa is moving so fast, leaving behind the regulatory regimes. Therefore moving forward, it may be better or beneficial if legislation is made after the innovation as this way, loopholes and irregularities can be identified and addressed.

Africa was not a key player in the first and second industrial revolution at all while in the third, there was a bit of participation in the revolution. Most importantly, Africa is actively participating in the fourth revolution.

AI and Robotics are Transforming Health Care in various ways:

These include:

- Keeping well
- Early Detection
- Diagnosis
- Decision making
- Treatment
- End of life care
- Research
- Training

Virtually everything now is driven by Artificial Intelligence (AI), which includes in the health sector, things such as medical wearables. These, together with the growing number of Internet of Things (IoT) surrounding us everywhere all play a role in data collection.

In fact,

We need to ask to move forward with it, but we also need to have very agile policymakers.

Agility is important because if we stand in the way, we would put back Africa where it was during the first industrial revolution.

mHealth applications and other digital medical devices have proven to be important as they help doctors make the right decisions and diagnoses.

Data collection and storage can aide in finding good solutions. For example, where there is a database of similar diagnoses, treatment may be simpler, easier and cheaper. What then needs to be debated is how such data can be collected and used while maintaining the datasets' privacy. A good way to do this would be by anonymising the data.

There are areas of mHealth Practice Areas in Africa that have vastly advanced. These are areas such as primary care services, radiology, oncology and pathology among others.

Africa's Infrastructure

The infrastructure in Africa on a general scope has also improved and can be advantageous in the health sector. Africa has both undersea and terrestrial fibre cables which advances connectivity within the continent. This way, collaboration is enhanced to improve patient care without the physician having to be there in person.

In this session, it was advised that Africa should find solutions in whichever way possible and then figure out how ethical measures will be construed into the solutions.

Embracing the Fourth Industrial Revolution (4IR)

Reasons why we must embrace 4IR:

- Global collaborations
- Greater efficiency in resource utilisation
- Cost-effective solutions
- Experts in Africa can offer services across borders
- High success in surgical procedures will lead to greater credibility for African doctors and surgeons
- Better telemedicine.

It is not easy to calculate the actual cost of having data collected. However, on a larger scale, the advantages seem to outweigh the costs.

In concluding this session, it was recommended that Africans should not worry about the regulations before perfecting the innovations. Therefore, we should

aim to perfect the innovations then consider the regulations affecting thereafter.

Final remarks:

In concluding the webinar, Professor Pamela Andanda, acknowledged the panellists' and all other discussants' participation. The main goals of the webinar were achieved and these were:

1. Engaging and identifying key stakeholders
2. An opportunity for fact-finding on the specific nature of challenges that affect the handling of health data when managing health apps. We need to interrogate the kind of policies that are there to protect personal data**. This should be driven by common sense.**
3. Found out various possible and important suggestions on managing and mitigating the challenges that emerged from the use of health data and how we handle that.

---

[1] https://www.odpc.go.ke/resources/data-protection-registration-of-data-controllers-and-data-processors-regulations-2021/

[2] https://www.odpc.go.ke/resources/data-protection-compliance-and-enforcement-regulations-2021/

[3] https://www.odpc.go.ke/resources/data-protection-general-regulations-2021/

[4] https://www.acronis.com/en-us/articles/nhs-cyber-attack/