Towards a Universal Health Data Sharing Policy for Uganda

End of Project Report

October 2023

Adroit Biomedical and Bio-Entrepreneurship Research Services Limited
P. O. Box 112139 Kampala
Naguru-Kampala
Email: grants@abbrs-uganda.org

Table of Contents

1.0 Background 9
1.2 Significance of Sharing Health Data 10
1.3 Methodology 11
2.0 Results of Policy Analysis 13
2.1 National Laws, Regulatory Frameworks and Policies 13
2.1.1 The 1995 Constitution of the Republic of Uganda as amended 13
2.1.2 The Access to Information Act, 2005 14
2.1.3 The Computer Misuse Act, 2011 as amended 14
2.1.4 The Data Protection and Privacy Act, 2019 14
2.2 Ministry of Health 16
2.2.1 National Guidelines for Research Involving Humans as Research Participants, 2014 16
2.2.2 The National eHealth Policy, 2016 16
2.2.3 The Ministry of Health Strategic Plan 2020 – 2025 17
2.2.4 Uganda Health Information and Digital Health Strategic Plan 2020 – 2025 (HIDH) 17
2.2.5 The National Health Policy, 2021 (NHP) 18
2.3 Ministry of Information Communication Technology and National Guidance Policies 19
2.3.1 The Information Technology Policy for Uganda, 2010 19
2.3.2 The National Electronic Government Policy Framework for Uganda, 2011 19
2.3.3 National ICT Policy for Uganda, 2014 19
2.3.4 Open Data Policy, 2017 20
2.3.5 Cybersecurity Strategy 2022 20
2.4 Subnational Policy Frameworks 21
2.4.1 Kampala City Council Authority Strategic Plan, 2020-2025 (KCSP) 21
2.4.2 Kampala City Council Authority Information Systems Strategic Plan, 2020-2026 (ISSP) 22
2.5 Academic Institutions 22
2.5.1 Makerere University Information and Communication Technology Policy 22
2.5.2 Makerere University Intellectual property management policy (IPMP) 23
2.6 Medical Research Organisations (MROs) 23
2.6.1 MRO 1 23
2.6.2 MRO 2 24
2.7 International Policy Frameworks 25
2.7.1 The Helsinki Declaration 25
2.7.2 EU General Data Protection Regulations 25
2.7.3 Global Data Facility 25
2.7.3.1 World Development Report 2021: Data for Better Lives 26

2.7.3.2 Cape Town Global Action Plan for Sustainable Development Data 27
3.0 Results of Key Informant Interviews 28
3.1 Control 28
3.2 Different processes 29
3.3 Centralisation 30
3.4 Privacy, Trust, and Accountability 31
3.5 Resources 32
3.6 Collaboration 33
4.0 Discussion 34
5.0 Recommendations 38
6.0 Conclusion 39
Appendix 1: Summary of the Report 40

Acknowledgements

The compilation of this report on the harmonisation of health data policies in Uganda was done by Adroit Biomedical and Bio-entrepreneurship Research Services (ABBRS), with financial support from DT Global and technical support from the Infectious Diseases Institute (IDI). The work started in May 2023 and was concluded in October 2023. The ABBRS team included Counsel Charles Reagan Mutyaba, Racheal Nereema, Salama Kasoga, Edrine Princess Kirabo, Dr. Emmanuel Musisi, Dr. Wilber Sabiiti, Dr. Abdulwahab Sessolo, Dr. Anne Nattembo, and Dr. Andrew Walakira. The team also acknowledges support from the various experts who reviewed the draft version of these reports. ABBRS expresses sincere gratitude to the government and non-government actors who shared policy documents, participated in interviews and the validation workshop.

Executive Summary

Efficient and secure sharing of health-related data is crucial for driving better clinical practice, research, innovations, and implementation of precise public health programmes such as routine vaccinations. Uganda, like many other countries, can greatly benefit from leveraging the vast amount of health-related data generated by different institutions. This report is about the gaps that hinder efficient sharing of health-related data as identified from the assessment of relevant data protection laws at national level i.e., the constitution of Uganda and Acts of parliament relevant to data management, and institutional policies from ministry of health, local government, and institutions involved in the medical research sector. The report also draws on interviews conducted with key stakeholders in data management at national, subnational and organisation levels to gain their insights and examine the challenges hindering sharing of health-related data. Gaps in data sharing laws, and policies exist at all levels of the healthcare system in Uganda. This study identified the following key gaps:

1. Levels of data sensitivity are not clearly defined in the law and policies, leaving it open for data holders to decide what is sensitive or not. For example, data holding agencies who are not willing to share data can easily cover themselves under clauses such as infringement on person's privacy, state sovereignty and national security clauses to deny data access to bonafide stakeholders.

2. The national laws do not effectively protect local institutions in the process of negotiating data management contracts. The laws leave this entirely to collaborating parties, in which case the local institutions are often the weaker party as they struggle to balance many competing interests including threats to lose funding if they take hard stance for equal data control.

3. Procedures for accessing and sharing health-related data differ significantly among institutions and stakeholders. This complicates data access and sharing process as it means going through different hurdles from one institution to another to access data.

4. Limited or absence of collaboration among data holding agencies which complicates universalisation of data access and sharing policies.

5. Limited commitment and/or policies to guide centralisation of data in data repositories in the country. Data repositories simplify data access because the parties seeking access will go through one process instead of multiple processes if data is held under different institutions.

6. Inadequate financial and human resources for data management making it difficult to have the infrastructure and experts needed for effective management.

To maximize the potential benefits of data, we recommend the following:

1. Streamlining the legal and policy framework to increase clarity on the freedoms and limitations to data access in the context of data privacy, consent, ownership, and data sharing agreements between institutions and other interested parties.

2. Establishing efficient data-sharing systems and platforms that are interoperable to allow seamless sharing of health-related data among different stakeholders. This includes implementing health information exchange systems that enable secure sharing of data between healthcare providers, research institutions, and other stakeholders.

3. Enacting policies to guide and promote collaboration among different stakeholders, including government agencies, healthcare providers, researchers, and industry partners. This will promote the harmonisation of data sharing/access standards, protocols, and governance frameworks to meet the needs and interests of the broader healthcare ecosystem.

4. Establishing robust ICT infrastructure through which data can be safely collected, stored, mined and/or shared with other parties.
5. Increase financial investment and human resource in data management in both public and private institutions.
6. Increase public engagement and awareness about the value of data and the rights and obligations of all stakeholders including the data subjects
7. It is essential to achieve a balance between privacy and data sharing. This can be achieved through efficient accountability to all stakeholders thus building trust in the entire data eco-system in the health sector.
8. Developing and implementing a national Health Data Strategy that considers all data management principles, legislation, rules, processes, and resources to drive policy development, practice and innovation. The process of developing this strategy should be multisectoral and involve all stakeholders in the healthcare system.

List of Abbreviations

ABBREVIATIONS	FULL FORM
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DHTs	District Health Teams
EGI	e-Government Infrastructures
eHMIS	Electronic Health Information System
EHR	Electronic Health Record
EMR	Electronic Medical Record
EU	European Union
EU-GDPR	European Union- General Data Protection Regulation
FAIR	Findable, Accessible, Interoperable, Reusable
GoU	Government of Uganda
HEI	Health Information Exchange
HIDH	Health Information and Digital Health
HIS	Health Information System
HMIS	Health Management Information Systems
HRIS	Human Resource Information System
HRHIS	Human Resources for Health Information System
HPT	Health Policy Triangle
ICT	Information Communication Technology
IPMP	Intellectual property management policy
IT	Information Technology
ISSP	Information Systems Strategic Plan
KCCA	Kampala Capital City Authority
KCSP	Kampala City Strategic Plan
LANs	Local Area Networks
LGs	Local Governments
M&E	Monitoring and Evaluation
MDAs	Ministries, Departments and Agencies
MDGs	Millennium Development Goals
MoH	Ministry of Health
MoICT	Ministry of Information Communication Technology
MROs	Medical Research Organizations
NCII	National Critical Information Infrastructure
NDC	National Data Centre
NGOs	National Governmental Organizations
NHDR	National Health Data Repository
NHP	National Health Policy

NITA-U	National Information Technology Authority – Uganda
PH&ED	Public Health and Environment Directorate
READ	Read Extract Analyse Distil
REC	Research Ethics Committee
SDG	Sustainable Development Goals
SOPs	Standard Operating Procedures
UNCST	Uganda National Council of Science and Technology
WAN	Wide Area Network
WHO	World Health Organization

Definition of Key Terms

Consent: means any freely given, specific, informed, and unambiguous indication of the data subject's wish, by a statement or a clear affirmative action that signifies agreement to the collection or processing of personal data.

Data: refers to recorded information in structured or unstructured formats, including text, images, sound, and video.

Data collector: is a person or an entity that collects data.

Data controller: is a person or entity who alone, or jointly with other persons/entities nor as a statutory duty determines the purpose for and the way by which data is processed or is to be processed.

Data processor: is a person/entity other than an employee of the data controller who processes data on behalf of the controller.

Data sharing: refers to the practice of making data available to others for various purposes, including analysis, research, collaboration, and decision-making. It involves providing access to data sets, information, or digital resources to individuals, organizations, or the public. Data sharing is a function of deciding what data, in which form, by what means and to whom it needs to be shared. Whereas data access refers to the function of providing access to the shared data to the correct entities.

Data subject: is an individual from whom or in respect of whom personal information has been requested, collected, collated, processed, or stored.

Health data: also referred to as health-related data, is any information about health. This includes information about health conditions, lifestyle factors, demographics, medications, treatments, behaviours, diagnoses, causes of death quality of life, patient health records, studies of the health of groups of people, test results (such as blood tests, x-rays, or scans) results from research studies and community-based health projects. Our focus in this study was on health data sharing.

Personal data: any information about a person from which the person can be identified and/or includes an expression of opinion about the individual.

Harmonisation: means adjustment of differences and inconsistencies among different laws, regulations, methods, procedures, specifications, or systems of medical products regulation to make them mutually compatible among different national or regional regulatory authorities.

Misalignment of laws/policies refers to situations where different laws, regulations, or legal frameworks are inconsistent or conflict with each other, leading to confusion, legal challenges, or unintended consequences.

Regulations: this refers to guidelines or procedures passed by a line minister as provided by enabling law.

1.0 Background

A lot of health data is generated everyday by different institutions in Uganda. If used efficiently, these data can drive better clinical practice, research, and innovations, and in turn yield benefits at various social and economic levels. To maximize the benefits, health data needs to be collected and processed efficiently, stored safely, shared easily and resourcefully among the different stakeholders without compromising its quality, the privacy and consent of the data source. This process needs to be guided by effective national laws and institutional policies. Misalignment of these policies can be a hindrance to efficient data sharing among institutions thus negatively impacting research and innovations in medicine. We reviewed the data related national laws plus data sharing policies of major institutions involved in medical research in Uganda to identify gaps and bottlenecks that prevent or hinder efficient and resourceful data sharing among stakeholders in the healthcare system in Uganda. The team further analysed how policies adhere to FAIR (Findable, Accessible, Interoperable, Reusable) data principles which are key to facilitating smooth and efficient sharing of data among key stakeholders. Efficient data sharing requires well aligned data sharing policies to facilitate this process.

Uganda has a robust health governance eco-system which is composed of both public and private health facilities and institutions. The public health sector includes all Government of Uganda (GoU) health facilities under the jurisdiction of the Ministry of Health (MoH). The public healthcare eco-system comprises decentralised health services managed by district health teams (DHTs) at the local government level, and Kampala City Council Authority Health team for Kampala capital city. The private healthcare system comprises of healthcare facilities (for-profit and not-for-profit), research organisations, implementing partners and development partners, and civil society organisations. All these components of the healthcare system generate essential data which if used maximally, can drive high quality clinical practice, research, innovations, and implementation of well targeted public health programs like mass vaccinations.

We recognise that vaccines are probably the most effective prevention strategy for various diseases in Uganda and other countries. Uganda routinely implements vaccination for 11 diseases including tuberculosis, polio, measles, mumps, tetanus, whooping cough etc while other vaccination campaigns are conducted on demand such as the recent COVID-19 vaccination. However, the use of vaccines to control the COVID-19 pandemic exposed various challenges in vaccine uptake by the public, putting a spotlight on the efficiency of vaccination programmes in the country. Furthermore, it highlighted the need for seamless sharing of health-related data to inform policy and decisions on disease control measures including deployment of resources for research and innovation. Hurdles experienced in sharing of COVID-19 pandemic data further highlighted the need to establish policies that ensure collection of high-quality data, and establishing standardised systems that enable FAIR data principles. For example, developing tools that allow findability and access, standardising the formats in which data is collected and stored facilitates interoperability, and these ultimately allow efficient sharing and reuse of data.

Beyond health data to inform public health policy and clinical practice, data is currently a centre piece for innovations in artificial intelligence (AI) and machine learning (ML), novel diagnostics, therapeutics and vaccine development. In short, data now has a monitory and business value attached to it. This further complicates the data access and sharing landscape as no one wants to be found to have missed the potential commercial benefits of the data. Questions arise on the ethics of deriving commercial benefits from data given freely by research and survey participants. The need for laws and policies to ensure equity and fair share in the benefits of data, cannot be more emphasised.

The legal and regulatory contexts in which health data is generated, shared, and used are important as they are key mechanisms that enable data exchange within and across organisations. This report

presents findings from the study that aims to examine the legislation, policy and regulatory frameworks that are relevant to health data sharing in Uganda. This is particularly significant because of the ability of health information systems to draw upon data from both the public and private health services, as well as non-health sectors. Health-related research funders, regulators, research and medical institutions, civil society organisations and relevant Ministries in Uganda increasingly need individual and community level health data widely to inform evidence-based decision making; yet the volume of data shared remains low. This report highlights the need to harmonise the legal, regulatory and policy frameworks to enable efficient data sharing among stakeholders at various levels of the system.

1.2 Significance of Sharing Health Data

Data is the engine that drives the present and the future of medicine and healthcare delivery. Access to high quality health data is a key driver of technology advancement in areas of public health, drug discovery, vaccine and diagnostics development, and digital technologies such as telemedicine, to mention but a few. Such developments in turn increase accurate disease identification, management, and eventual reduction of disease burden. It is thus important to facilitate seamless and efficient sharing of health data within and among institutions both locally and internationally. This is only possible if health data sharing policies of local institutions are well aligned with one another, and with national and management policies will enable achievement of sustainable development goal (SDG) 17 which aims to strengthen and revitalise global partnerships by enabling international cooperation in science, technology, innovation and thus enhancing knowledge sharing on mutually agreed terms.

Efficient data sharing policies make data accessible thereby increasing the chances of novel innovations to ensure good, health for all (SDG 3). The COVID-19 pandemic highlighted this need since sharing data was critical in developing both the vaccine and other interventions that were used to control this disease. Efficient sharing of data on vaccines is critical to improving vaccine uptake in communities. If data on vaccines is shared appropriately, the masses get the facts thereby avoiding misinformation; authorities are able to channel the right vaccines in the right amounts to the right people, and adverse effects due to vaccines are dealt with efficiently. As a result this builds trust among the public which in turn increases vaccine uptake. Furthermore, sharing data enables fair representation of different communities and their unique medical characteristics leading to development of medical interventions tailored to benefit people of various races, and ethnic backgrounds. Sharing data also leads to the identification of rare and geographically localised diseases more so among people living in resource limited settings.

Therefore, a lack of effective data management policies or a presence of policies that conflict with each other at the different layers of society hinders FAIR data principles thus making it difficult to find and access data. This limits the benefits of medical research. To address this problem, the study aimed to explore the landscape of data management policies in Uganda, internationally and make recommendations for harmonization, and advancement of FAIR data principles. We believe the outcome of our research will lead to the development of coherent data management policies that enhance efficient data sharing within and among institutions. We aimed to review policy documents to identify gaps and opportunities to strengthen health data sharing within and across the different levels as shown in Figure 1 (see page12). Figure 2 (see page 13) illustrates the project methodology, results, and significance. It shows that by using the multidimensional health policy analysis framework, complimented by the FAIR data principles, we were able to conduct an in-depth analysis of the health data sharing policy environment through document review and interviews. We identified the key gaps and recommendations. If these recommendations are adopted, they will contribute to efficient and effective health data sharing, comprising of various data categories from a range of sources to facilitate decision making for improved health outcomes.

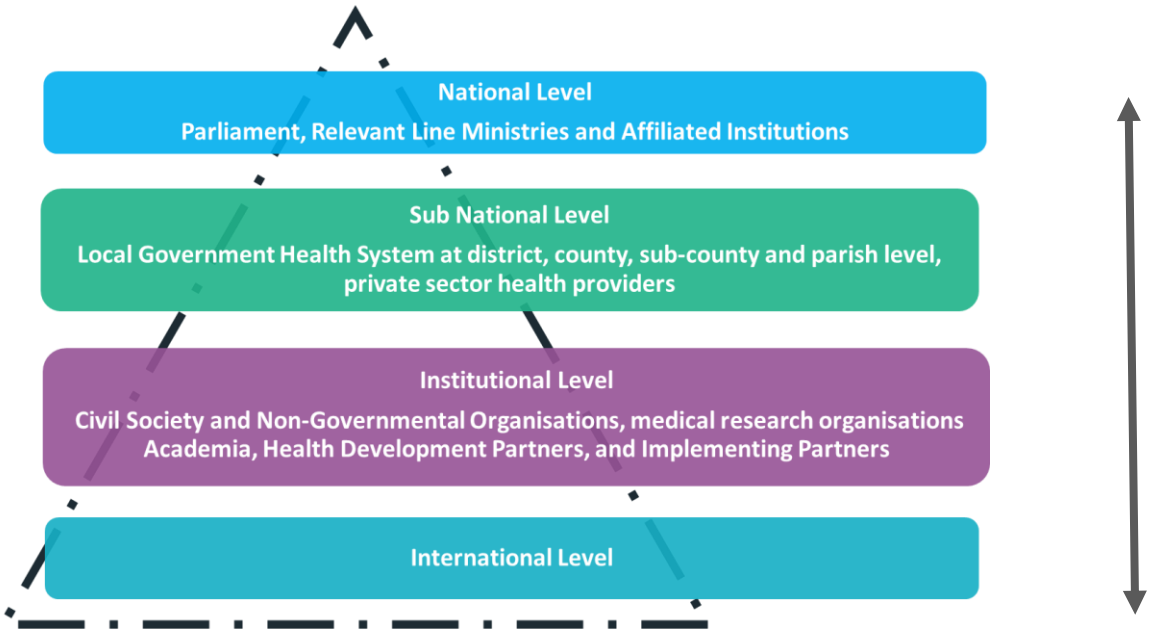


Figure 1: Data sharing policy development and health data sharing structure

1.3 Methodology

We conducted a document review with a qualitative approach to analysis. A document review approach allowed for an in-depth examination and interpretation of data to elicit meaning and gain an understanding of health data sharing. Using a document review approach was informed by our aim to identify clauses that speak to data sharing in various relevant Ugandan policies either specifically or in an inclusive manner. The policies included the Constitution of Uganda, relevant Acts of Parliamentary, Ministry of Health strategic plans, guidelines and training manuals, relevant policies from Kampala City Council Authority, Makerere University and Medical research organisations. We identified relevant documents firstly from institutional websites such as the parliament library and ministry website. Secondly, we contacted the departmental designated contact persons in the Ministry of Health, Kampala City Council Authority, Makerere University. These institutions were selected because they play a key role in data generation.

Herein, we considered a policy document as an action plan or a guideline that contains the intention of a government or institution concerning data sharing. The following policy types were included, the Constitution of the Republic of Uganda, Acts of Parliament, frameworks, agreements, implementation plans, strategic plans, operational plans, action plans, strategies, roadmaps, policies, program guidelines, and program plans. The team developed a policy analysis matrix to facilitate analysis of the documents judgements about the quality and potential of a policy to address data sharing. It was developed on the assumption that intended outcomes of public policies are more likely to be achieved if the policy issue is well-defined, specific goals and actions are stated, sufficient resources are allocated, and policymakers are accountable through monitoring mechanisms and most importantly, that the policies complement each other rather than conflict.

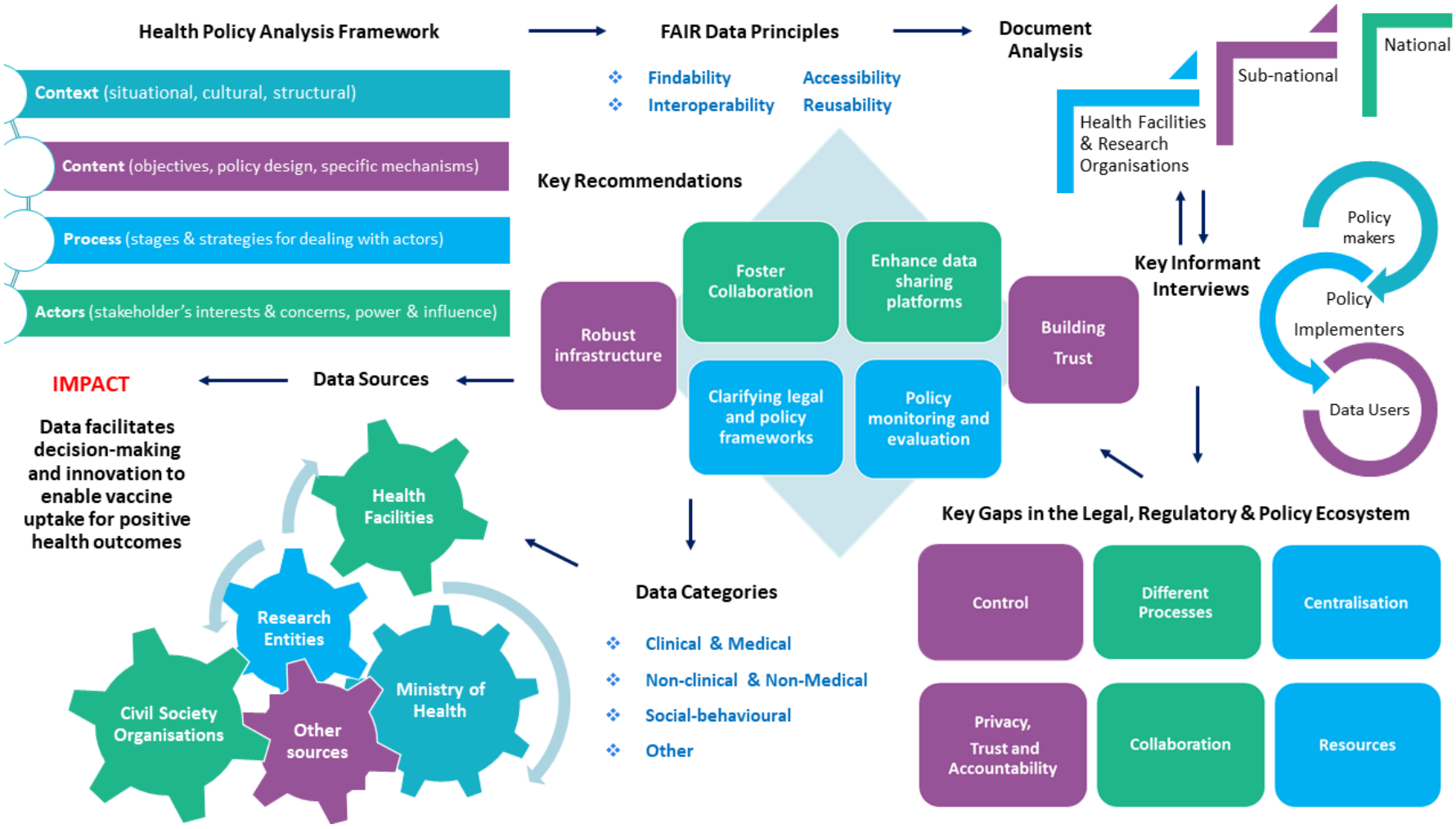


Figure 2: Summary of the project methodology, results, and significance.

2.0 Results of Policy Analysis

From this study, we find that at all levels (i.e., international, national, and sub-national) of the health service delivery structure, the policies analysed in this document analysis indicated that the definition of data sharing remains non-specific, and, in some policies, data sharing was not mentioned. Secondly, FAIR data principles were rarely mentioned or implied in the policies. In instances where the principles were mentioned, the description was not comprehensive enough to guide action. Several people at these institutions are involved in the data eco system and thus impact the flow and management of these data. There are also people who are not directly involved in the collection or management of health data yet influence the laws and policies that govern these data. These key persons influence the content of the data management policies, implement them, and determine who can access the data. The sections that follow provide more details based on the findings from the documents at different health service delivery governance levels as well as the challenges experienced in implementing data sharing policies.

2.1 National Laws, Regulatory Frameworks and Policies

Access to high quality data is a requirement for evidence-based decision making, which ensures efficient service delivery to society including public health. It is thus important to ensure a seamless flow of data to support decision making research and innovations. Uganda, like any other country, has a set of laws and policies at national, subnational, and various institutional levels that address how data should be managed and shared.

2.1.1 The 1995 Constitution of the Republic of Uganda as amended

The Republic of Uganda has a constitution which is the supreme law of the land. Article 27 gives citizens the right to privacy, and this means that an individual chooses which of their personal data can be released to third parties. In article 41, the constitution gives citizens the right to access information held by government provided the information does not compromise security, state sovereignty and where it does not infringe in the person's right to privacy These articles can be applied to health data but cannot stand alone for the purposes of sharing such data. The constitution catered for this by mandating the parliament to enact additional laws for access and management of data.

Article 27 states that "no person shall be subjected to; (a)(i) unlawful search of the person, home or other property of that person, (ii) unlawful entry by others of the premises of that person, and (b) no person shall be subjected to interference with the right to privacy of that person's home, correspondence, communication or other property."

Article 41 provides for the right of access to information, and it states that, "(i) every citizen has a right to access to information in the possession of the state or any other organ or agency of the state except where the release of the information is likely to prejudice the security or sovereignty of the state or interfere with the right to the privacy of any other person." Subsection (ii) of this article states that, "parliament shall make laws prescribing the classes of information referred to in clause (i) of this article and the procedure for obtaining access to that information."

2.1.2 The Access to Information Act, 2005

In 2005, the parliament of Uganda enacted the Access to Information Act which detailed the type of information/data to which article 41 of the constitution applies. We deduce that information held by MoH is directly impacted by this Act and Article 41 of the constitution. The Act does not exclude medical records held by government in public health facilities. However, it affirms that the accessed information should not infringe on the privacy of an individual, state sovereignty and national security This may mean that an individual can access medical records that have been anonymised.

Section 2 (1) states that "this Act applies to all information and records of Government ministries, departments, local governments, statutory corporations and bodies, commissions and other Government organs and agencies, unless specifically exempted by this Act. This Act does not apply to, a) Cabinet records and these of its committees; b) records of court proceedings before the conclusion of the case."

Section 5 states that, "every citizen has a right of access to information and records in the possession of the state or any public body, except where the release of the information is likely to prejudice the security or sovereignty of the state or interfere with the right to the privacy of any other person."

Section 8 refers to the availability of data, and it states that, "An information officer shall, once in two years, publish a description of:- a) the categories of records of the public body that are automatically available without a person having to request access under this Act, including the categories available;- (i) for inspection under a written law other than this Act; (ii) for purchase or copying from the public body; and (iii) from the public body free of charge; and (b) how to obtain access to those records." Section 21 limits access to health or other records, "an information officer shall refuse access to health records, the disclosure of which would constitute an invasion of personal privacy."

2.1.3 The Computer Misuse Act, 2011 as amended

Section 3 states that, "A person secures access to any program or data held in a computer if that person: - (a) views, alters or erases the program or data; (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; (c) uses or destroys it; or (d) causes it to be output from the computer in which it is held whether by having it displayed or in any other manner." The Act facilitates data sharing that, "Access by a person to any program or data held in a computer is authorized if:- (a) the person is entitled to control access to the program or data in question; or (b) the person has consent to access that program or data from any person who is charged with giving that consent." Furthermore, the Act works to prohibit unlawful disclosure of data as described in section 18 (1) which states that, "except for the purpose of this Act …, a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access."

2.1.4 The Data Protection and Privacy Act, 2019

The Data Protection and Privacy Act of 2019 further clarifies on the grey areas from previous laws. It mainly aims to establish a framework for protection of personal data, and it applies to both public and private entities in Uganda. This act distinguishes between data collector (entities that collect the data), data controllers (entities that determine the purpose and means of processing personal data) and data processors (entities that process data on behalf of data controllers), elaborates their responsibilities and

the rights of data subjects. In some situations, the data collector, controller, and processor are the same entity.

Section 3 (1) that provides for principles of data protection by stating that, “A data collector, data processor or data controller or any person who collects, processes, holds or uses personal data shall:- (a) be accountable to the data subject for data collected, processed held or used; (b) collect and process data fairly and lawfully; (c) collect, process, use or hold adequate, relevant and not excessive or unnecessary personal data; (d) retain personal data for the period authorized by law or for which the data is required; (e) ensure quality of information collected, processed, used or held; (f) ensure transparency and participation of the data subject in the collection, processing, use and holding of the personal data; and (g) observe security safeguards in respect of the data. ”

Section 4 of the Act establishes the data protection office. Subsection (1) states that, “There is established a personal data protection office responsible for personal data protection under the Authority which shall report directly to the Board.” The “Authority” being referred to here is the National Information Technology Authority-Uganda (NITA-U), which itself is stablished under the MoICT. In Section 5, the Act mandates the personal data protection office to 1 (a) “oversee the implementation of and be responsible for the enforcement of this Act”, (c) “monitor, investigate and report on the observance of the right to privacy and of personal data.” Subsection 2 empowers this office to fulfil its duties as defined in the Act, “The office shall have all powers necessary for the performance of its functions under this Act.”

Section 6 provides for a Data Protection Officer where it stated that, “for purposes of this Act, and in so far as it applies to an institution, the head of the institution shall designate a person as the data protection officer responsible for ensuring compliance with this Act.”

Section 19 provides for processing personal data outside Uganda and it avers that, “where a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller shall ensure that: - (a) The country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by this Act; or (b) The data subject has consented.”

However, in other situations such as research collaborations, the data collector may not necessarily be the data controller. In such a situation, the data controller (who is most likely to be the funder, or an entity assigned by the funder) may decide to choose another entity as the data processor. This becomes a very complex relationship (as regards to data management) with complicated power dynamics. Here is when we are reminded that a lot of scientific research in Uganda is funded by foreign partners, and hence they would assume the position of data controller. There is an unequal balance of power between local and foreign partners in which case foreign partners tend to have more power and control over the data. This causes challenges on how local stakeholders and researchers may access, share, and use data from research projects. The Act instructs the establishment of Data Protection Officers in organisations that meet the criteria and assigns them the power to decide which data can be shared and with whom. This does not help resolve the challenges above because an officer employed and renumerated by a private organisation is unlikely to authorise the release of data to other stakeholders against the wish of their employer even when it’s for public good. It is important that all stakeholders realise that data subjects voluntarily give their data for defined objectives, broadly for the improvement of health for all. Their participation, by law or by ethics, is not paid or induced by money or gifts. As such, funding the process of data collection does not automatically give the right of ownership to these data. The right to ownership, and thus access to these data should be fair and balanced among all stakeholders with the general objective of improving health for all.

2.2 Ministry of Health

The MoH is directly responsible for the smooth operations of health activities in the country. The ministry produces policies, guidelines and strategic plans to enable it to achieve its objectives. In 2014, the MoH produced guidelines for conducting research involving humans. These guidelines left the issue of data ownership to the collaborating parties to decide at project inception. This is a challenge as it leaves local institutions unprotected in the process of negotiating collaboration contracts.

2.2.1 National Guidelines for Research Involving Humans as Research Participants, 2014

Section 11.1 states that "data ownership and associated intellectual property rights shall be discussed and agreed upon by collaborating partners at the inception of a research project. Collaborating research partners shall negotiate data ownership and use in accordance with the host organization's data use and ownership policies. Ownership of data shall be clearly stated in the research protocol or collaborative research agreements, which shall be reviewed by the REC and registered with UNCST." Section 11.2 states that, "(a) collaborating research partners shall agree on appropriate data access and use rights before commencement of the study. Researchers shall have in place mechanisms for maintaining confidentiality of research participants and their communities. (b) A collaborating research partner shall not transfer data to a third party without the written consent of the other partner. (c) Local researchers shall have unrestricted access rights to data sets collected through a collaborative research project. (d) Researchers shall ensure that research records from which the data has been obtained are available at the research site for at least five years after completion of the research project. Electronic records are acceptable."

2.2.2 The National eHealth Policy, 2016

Section 7.3, the policy aims "to establish eHealth services and tools that address the priority business needs and to facilitate the establishment of a process of authorization, sharing and managing electronic data, information, knowledge, and practices between organizations and stakeholders in the health industry including patients/clients, healthcare providers, and healthcare managers." The policy further identifies policy strategies as; "Policy Strategy 1: Establish a unique, standardized, comprehensive and comprehensible Electronic Medical Record (EMR), Electronic Health Record (EHR) and Personal Health Record (PHR). Policy Strategy 2: Establish a comprehensive health facility, provider, and client registries with complete and current information that meets stakeholders' needs. Policy Strategy 3: Establish, prioritize, and implement eHealth Services in line with the eHealth Enterprise Architecture and Interoperability Framework Policy; Strategy 4: Develop and operationalize an eHealth Data Management and Utilization System across all levels of healthcare. Policy Strategy 5: Align Health Data management and Utilization to other existing government laws and regulations."

Section 7.4 facilitates the "establishment and sustainability of ICT Infrastructure and connectivity to support the effective delivery and monitoring of eHealth as an enabler of better healthcare services. This shall include all the components of infrastructure which are computing infrastructure, databases, directory services, infrastructure development & management, connectivity, and storage. This also includes complementary infrastructure like power and buildings." In section 7.4.3, the policy aims, "Policy Strategy 1: Connect all priority health facilities to the National Backbone and the National Data Centre with a view of having secure, reliable and affordable data connectivity and internet services," and, "Policy Strategy 8: Ensure that ICT Infrastructure is established in a coordinated manner and meets the standards with guidance from MoH in conjunction with MoICT and NITA-U."

Section 3.1.3 states that, “there are some eHealth services being implemented across the health sector such as the Health Management Information Systems (HMIS), DHIS2 and Human Resources for Health Information System (HRHIS) among others. The MoH has a Knowledge Management Portal; an online resource that integrates health and health related information resources from the Ministry of Health and beyond. This provides a single point of access to valuable information that facilitates evidence-based decision making.” This is a noble effort to make data more accessible. However, this resource may not include data from private institutions such as MROs. The MoH acknowledges the importance of partnerships as referenced in section 3.1.11, “A National Policy on Public-Private-Partnership in Health4 was developed to provide guidance to mainstreaming, establishing, implementing, coordinating, monitoring and evaluating partnerships between the Government of Uganda and the private health sector within existing laws, policies and plans.”

2.2.3 The Ministry of Health Strategic Plan 2020 – 2025

Section 2.0.2, the document asserts that the previous plan aimed to, “enhance evidence-based decision making by establishing a culture that uses “big data” for improvement” of services. The plan further states in section 2.3.7 that, “there is a well-established and functional system for collection, processing, storage, retrieval and dissemination of health information for decision-making despite some challenges.” The section further identifies the “lack of repositories or “one stop-shop’’ that facilitate timely access to well indexed evidence.”

Section 2.1.3 that, “The sector has made progress towards aligning the previously fragmented information systems within the health sector to ensure contribution to the one M&E system.”

Section 3.6, Table 8, the document mentions the interventions and action plans for the specified period. It specifically mentions in subsection 1.9 the there is a plan to “strengthen data collection, quality and use” by “data analysis, synthesis and sharing of health information products including dashboards, bulletins/newsletters” and “update and maintain the National Health Data Repository.”

Subsection 7.6 aims for, “Digitalization of the HIS” through “stakeholder engagement, development and operationalization of the National Health Information Exchange Registries (Client, Health Workers, Health Facilities and Health Product)” In section 6.2 (4), the document further aims at “establishing a comprehensive Health Communication Knowledge Management System to facilitate standardized reporting, information sharing, and access to learning and vital resources.”

2.2.4 Uganda Health Information and Digital Health Strategic Plan 2020 – 2025 (HIDH)

HIDH developed strategies that enable data sharing and implementation of FAIR data principles. Strategy 1.6 aims to “improve data security and disaster recovery to ensure continuous access and availability of health data as well as compliance to Data Protection and Privacy Act. A comprehensive data warehouse for health data will be generated from all available sources including routine surveys as well as operations. MoH will thus use this resource to strengthen patient access to personal medical records as per the MoH Patient charter.”

Strategy 3.3 aims to “institute digital tools in the health sector that are interoperable and support the exchange of data/information in a coherent, secure and consistent manner.”

Strategy 4.1 aims to develop ICT infrastructure “composed of physical and virtual resources that support the flow, storage, processing and analysis of data.”

Under strategy 5.2, HIDH plans to “functionalise the health data collaborative as a platform that promotes sharing, joint planning and monitoring.” In strategy objective 6, HIDH plans to “ensure a functional collaborative mechanism to support health information and digital health implementation research and innovation by 2025.”

2.2.5 The National Health Policy, 2021 (NHP)

Section 3.6.6.1, policy objective 1 aims to, “ensure timely availability, accessibility, of quality health information for use in decision making, programme development, resource allocation and management at all levels and among all stakeholders.”

Subsection 1.2 states that “The health sector shall promote the use of evidence for policy and decision-making on the health system and interventions.”

Subsection 1.4, the policy commits that, “Ministry of Health shall establish and maintain a national Knowledge Management Portal to support knowledge translation efforts (such as one-stop shops for evidence) to promote access and use of health information for decision-making at all levels to improve health policy and system. This includes ensuring that all unit data of major publicly funded surveys related to health, are available in public domain in a research friendly format in line with the National Data Use Policy.”

Subsection 1.5 states that, “the health sector shall develop and scale-up the integrated eHMIS to strengthen timely and reliable statistics from both public and private health facilities and community level.”

Subsection 1.7 states that “the health sector shall strengthen multi-sectoral collaboration to improve data security and ICT infrastructure maintenance for management of health information.”

Subsection 1.9 states that the “Ministry of Health shall develop and institutionalize the national health information architecture by creation of registries (i.e., patients, provider, facilities, service, diseases, document and event) for enhanced public health and big data analytics, creation of health information exchange platform and national health information network.”

The ministry is making efforts to digitise data in its custody hence facilitating easy access and sharing of these data. In Uganda, data in digital form, hence held on computers, is directly impacted by the Computer Misuse Act of 2011 as amended. This Act, under section 5 (a) authorises the MoH, as the controller of the data it holds, to share the said data with third parties if that data is held on a computer. In section 18 (1), the Act bars unlawful disclosure of the data if the data is to be used for any other purpose other than for which it was obtained. The definition of “purpose of obtaining data” may differ between subject and entity. To the individual going to seek health services, the data is being collected for “diagnostic/treatment purposes.” To the MoH, the entity collecting and controlling the data, the data is obtained for “diagnostic/treatment of the individual and understanding the public health dynamics in the community.” Together with the Data Protection and Privacy Act 2019, that seems to authorise the MoH to share any data in its custody with third parties provided it has been anonymised. However, even after anonymization, some forms of health data such as genomics data can potentially be used to re-identify an individual for example through platforms like platforms like 23andMe and Ancestry DNA. These kinds of situation require special attention in the legal framework.

The MoH has produced other guidelines, plans and policies that aim to establish structures (including ICT) that could facilitate efficient handling and sharing of health data. The most notable is the division of Digital Health Information which is mandated to guide the ministry in this endeavour. To achieve efficient

sharing of health data, the MoH will require a robust ICT infrastructure. This can be achieved in collaboration with MoICT.

2.3 Ministry of Information Communication Technology and National Guidance Policies

The MoICT is mandated to establish and maintain the national ICT infrastructure to support both public and private initiatives. The MoICT has several policies and work plans aimed at achieving this objective. Indeed, there are tremendous gains in this direction. However, to maximise this potential for the benefit of the healthcare system, the MoICT has to work with MoH so as to customise products that cater for the unique requirements of health data. The documents reviewed show that the MoH acknowledges this need and has tried to bridge with MoICT to get more precisely targeted support.

2.3.1 The Information Technology Policy for Uganda, 2010

Section 1.5.5 mentions that ”the policy objectives are; of the document is to develop a harmonized national IT infrastructure that provides equitable access to foreign and local ICT resources markets, to provide leadership, direction and vision to guide IT industry development, to develop a critical mass of educated IT human resource at all levels to meet the local and export requirements, to stimulate and support research and design in IT development, to promote widespread use of IT applications in both public and private sectors to enhance efficiency and effectiveness in service delivery, to develop national and adopt international standards and guidelines to support growth of IT industry in Uganda, to develop an enabling legal and regulatory framework, to establish incentives for both local and foreign investors to foster the development of the IT sector (hardware, software and service industry), promote use of IT systems in all government Ministries Departments and Agencies(MDAs), and local governments (LGs) and businesses to usher in efficiency and effectiveness in-service delivery, and to mobilize and sensitize the communities on availability of IT services.”

2.3.2 The National Electronic Government Policy Framework for Uganda, 2011

Section 1.2, states that, “to“…a national e-Government programme aimed at the efficient use of ICT in public administration in order to improve public service delivery and democratic processes and also to enhance the attainment of the Millennium Development Goals (MDGs). promote efficiency, transparency, and accessibility of government resources using ICT to improve public service delivery, democratic processes and to enhance the attainment of the Millennium Development Goals (MDGs).”

Section 2.5.1.1 (v) the National e-government framework 2011 “highlights the establishment of a National Data Centre to facilitate government-wide data storage, usage, sharing, and security has been built”. Section 2.5.2 states that, “Government agencies are establishing Local Area Networks (LANs) to be interlinked to form the Government Wide Area Network (WAN) to facilitate the sharing of equipment, systems and human resources. The Nationwide Data Transmission Backbone (NBI)/ e-Government Infrastructures (EGI) installation across the country is ongoing for this purpose.”

2.3.3 National ICT Policy for Uganda, 2014

Section 41.4.1 mentions the need “to ensuring universal access to basic ICT infrastructure and services, providing enterprise-oriented and consumer-centric services.to ensure universal access to basic ICT

infrastructure and services, including the promotion of enterprise-oriented and consumer-centric services."

It further mentions Section 4.5.7 (C), states the principles on that, set up of electronic libraries with on-line linkages to reputed scientific information repositories, accessible to all major towns in the country to ensure economical and equitable access to world class information and publications.

Section 5.2.1.1 of the policy emphasizes "Promote the development and use of open source software, and building applications that are based on open standards the need to promote the use of open standards and protocols to ensure interoperability between different ICT systems and applications" and also enables "Implement the National data bank; Implement electronic document/record management system across government, the implementation of a National Data bank and electronic document/record management systems across governments to ensure that data is stored in a standardized and interoperable format."

In section 5.2.8 (c), the policy mentions the "need "to promote the use of peer-to-peer technology to share scientific knowledge and pre-prints and reprints written by scientific authors who have waived their right to payment which can help make scientific information more accessible to a wider audience."

This policy emphasizes, under Section 5.2.8 (d), "the long-term systematic and efficient collection, dissemination, and preservation of essential scientific digital data for example, population and meteorological data in Uganda and in Section 5.2.8 (e), "the need to promote principles and standards of metadata to facilitate cooperation and effective use of collected scientific information and data as appropriate to conduct scientific research."

2.3.4 Open Data Policy, 2017

Section 4 (iii) aims to "Establish an open government data portal that shall provide online public access to authoritative versions of government sanctioned open data."

Section 5 of the policy states that "The Office of the Prime Minister (OPM) shall lead the overall national coordination of the implementation of the Open Data Policy and shall lead the monitoring of the MDAs' implementation of the Open Data policy actions with support from the Ministry of ICT and NG."

Section 6.7 mandates The National Information Technology Authority – Uganda (NITA-U) to, "(a) Establish a centralized online portal to provide a single listing of all available open data, (b) Provide Data Hosting Services for Agency Data Sets, (c) Initiate partnerships with developers and innovation hubs to begin to unlock the economic value of open data in Uganda, (d) Issue the Government Enterprise Architecture and Interoperability Framework for utilization to maintain Interoperability, data standards and processes related to data management, (e) Ensure that MDAs use open standards to publish their data."

2.3.5 Cybersecurity Strategy 2022

In section 3.32.42, the Cybersecurity Strategy 2022-2026 mentions data sharing in the context of information sharing and incident reporting. It states that, "Update of the minimal cybersecurity baseline for National Critical Information Infrastructure (NCII) operators. Based on international standards and best practice, Government of Uganda (GoU) will enhance the implementation of security measures of NCII operators based on the regular risk assessments. To achieve the goal, the Government will set legal requirements for minimum cybersecurity baseline of NCIIs. The standard includes the requirements for information sharing and incident reporting.

Section 3.6.4 mentions that “Appropriate information sharing mechanisms (requirement for the private and public sectors) will be established through legal measures and appropriate protocols through the Uganda National Computer Emergency Response Team (CERT) and Coordination Centre”.

Section 3.2 shows that the policy aims to, “Strengthen national and sectoral Computer Security Incident Response Team (CSIRTs) and Develop tools for information sharing to create a minimum cybersecurity baseline for National Critical Information Infrastructure (NCIIs), appropriate information sharing mechanisms will be established through legal measures and appropriate protocols through the Uganda National Computer Emergency Response Team (CERT) and Coordination Centre. The mechanisms will ensure that information is shared in a timely, accurate, and secure manner. The Government of Uganda will establish a framework for incident reporting and response, which will include the establishment of a National Cybersecurity Incident Response Team (CSIRT) to coordinate the response to cybersecurity incidents." Generally, the ICT Ministry facilitates data sharing by setting up and maintaining ICT infrastructure through which data can be shared.

2.4 Subnational Policy Frameworks

Beyond the national level, we examined policies and the legal framework at subnational level (local government). We examined policies, plans and bylaws from KCCA since the study looked at institutions headquartered in Kampala district. Furthermore, KCCA is responsible for district healthcare facilities within its area of jurisdiction. It’s also important to note that KCCA enjoys a special administrative status as an “authority”, something unique among local governments in Uganda. Both the Kampala City Strategic Plan 2020 – 2025 and Information Systems Strategic Plan 2020-2026 aim to improve ICT infrastructure in the city. KCCA has made tremendous steps to achieve this including establishing a modern data centre. This is promising as pertains to enabling data sharing.

2.4.1 Kampala City Council Authority Strategic Plan, 2020-2025 (KCSP)

The “Strategic Goal” of the Kampala City Strategic Plan 2020-2025 is that “By June 2025, Kampala will be an inclusive, liveable, resilient, and well-planned City that provides economic opportunities.” Four thematic areas have been identified and prioritized which are City Economic Growth, KCCA Governance and Citizens engagement, Enhanced Quality of life and City resilience along with 21 Strategic Objectives, and 33 Sub Programs to guide the city development agenda for the next five years. Under the Quality-of-Life theme, KCCA aims to improve Public Health and Environmental management. However, the plan for management and sharing of health data is not clearly articulated.

The issue of data management and sharing comes out well under the city resilience theme. Here, KCCA plans to develop “the online KCC Data platform for sharing spatial data within KCCA, and externally with MDAs, NGOs, Academia, the Private Sector and all Citizens; this will include different levels of corporate and public access to the National Land Information System, for KCCA.” Spatial data is very relevant in health management, more so if it’s well aligned with prevailing public health challenges.

Over the next five years, KCCA plans to become “an institution that enhances City service delivery, solves its core issues through innovation and collaboration, and that applies new technologies and data for the benefit of all.” This is in line with the Information Systems Strategic Plan 2020/2021-2024/2025 that aims to improve the use of ICT in the management of the city.

2.4.2 Kampala City Council Authority Information Systems Strategic Plan, 2020-2026 (ISSP)

ISSP was developed with support from the National Information Technology Authority Uganda (NITA-U), and it mainly focusses on "empowering data-driven decision making, engaging stakeholders with relevant and timely information." This plan establishes what was termed as "The KCCA SMART City" initiative. This document asserts that the ICT department has "registered key achievements in the previous years which include among others; the implementation of a modern data centre for consolidation of all application hosting and data storage."

The ISSP is focused on establishing and improving ICT infrastructure and use in city operations and activities. However, the ISSP is silent on storage and management of health data in the city. During our interviews, we will make the effort to understand how the ICT infrastructure will be applied within the healthcare system of the city.

From the analysis, KCCA does not show its plan for health data in general and sharing of the data. However, KCCA has an elaborate plan for the handling of spatial data, mainly for the purpose of urban planning. Spatial data is also relevant in health and so can be of benefit to public health initiatives. Generally, KCCA plans to improve on ICT infrastructure and use in its operations around the city. This could enable sharing of health data if its considered a priority. Also, KCCA is interested in establishing collaborations with other stakeholders involved in research and academia. This too can facilitate sharing of health data.

2.5 Academic Institutions

Academic institutions are major stakeholders in the healthcare system of Uganda. These not only train personnel who work in this sector, but also participate in research either individually or as collaborators with other research institutions. Makerere University is one such academic institution that has established strong collaborations with major research institutions in the country and has participated in several endeavours of public health benefit. For this reason, we examined publicly available policies and documents from Makerere University to gain insight into its approach to data sharing.

2.5.1 Makerere University Information and Communication Technology Policy

The main objective of this policy is to provide for the centralized effective governance of all ICT related matters within the University in a rationalized and harmonized manner. The policy aims to provide effective ICT support that is responsible to the academic, research and administrative functions of the university. The policy guide on how ICT infrastructure of the university can be accessed and used. It also tackles matters of cyber security. The policy states that, "the University shall establish and maintain a Data Centre to act as the only central repository for all university databases and web hosting." The policy also aimed to harmonise the various information systems to avoid duplication of data and resources by enabling "Data Warehousing for Makerere University to achieve centralized management of information systems within a central data repository." This would also facilitate "interoperability between university information systems".

This policy affirms the availability of ICT infrastructure meant to enable university operations. It also defines how ICT facilities can be accessed. The policy is not categorically clear on how data can be shared. However, the policy establishes the necessary infrastructure to enable sharing of data with stakeholders.

2.5.2 Makerere University Intellectual property management policy (IPMP)

The policy aims to protect research, research outputs, and innovations. The purpose is to assist researchers, research managers and the university in ensuring that they have access to best practices for the identification, protection, and management of intellectual property and, therefore, to maximise the benefits and returns from public investment in research. In this policy, field data, databases, and data from third parties are considered intellectual assets.

The policy aimed to "develop an inventory/database of all research activities and innovations," (section 3.1.1). Subsection (iii) goes on to state that, "Research Reports including theses or dissertations approved for the award of University Degrees or Diplomas shall constitute intellectual assets and shall be deposited with the Makerere University Library and the National Library upon protection under the relevant law shall be transformed into intellectual property."

The policy establishes an Intellectual Property Management Unit, which in section 3.2.1 (iv) is tasked to "receive copies of Laboratory Notebooks and Asset Identification Forms for purpose of maintaining an inventory thereof." This is critical data. Subsection (j) adds that the unit should, "design and review periodically an Intellectual Property Data Management System for the University." The policy enables data sharing in many ways such as ensuring a central repository, storing some materials with the national library, and establishing structures that facilitate access.

The university has enacted policies aimed at improving ICT infrastructure within the university, and clearly assigning an authority, The Directorate of Research and Graduate Training, to handle all matters of research in the university including data management. There are structures that enable one to access and sharing data within the university if one is a member of the university (student or staff). However, it was not clear how the university handles the issue of data sharing outside the university, more so with its collaborators. It is likely that this is handled on a case-by-case basis for each collaboration agreement.

2.6 Medical Research Organisations (MROs)

We contacted eight (8) MROs and requested for access to their data management and sharing policies. Gaining access to these policies involved many procedures. We acknowledge that it was a highly bureaucratic process, way more than we anticipated. We replaced the name of the MRO with *"MRO-institution"* for purposes of confidentiality.

2.6.1 MRO 1

This is a policy in draft. Section 2.1 identifies its objective as, "these guidelines serve to advance the value of *"MRO-institution"* data as an institutional resource and to facilitate access so as to support clinical care, training and research while avoiding inappropriate use".

Regarding data sharing, the policy in Section 2.0 states that ".... This can be used to improve service delivery". The three closely related principles regarding data are it is an asset; it is shared and easily accessible. Individual patient clinical data, lad, pharmacy etc. that can be used for research, publications, patient clinical monitoring, advocacy, developing reports to MOH, donors and other stakeholders, academic advancement, and academic evaluation".

Section 2.0 mentions "In the rationale for this policy, it serves as a guideline for persons wishing to access data collected by *"MRO-institution"* at any of its implementing sites for purposes of career development, research, evaluations, conference presentations, advocacy, publications, and other uses. The policy shall apply to all persons involved in the design, conduct or reporting of research/work leading to presentations or publications with the use of *"MRO-institution"* data resources of facilities. It shall apply to all projects on which those individuals work regardless the sources of funding of the project". Section

2.0 further states that "the *"MRO-institution"* data is owned by *"MRO-institution"* under the school (Formerly faculty) of medicine Makerere University. The stakeholders (Mulago hospital, Mbarara Hospital and Mbarara Faculty of Medicine, Regional Referral Hospitals and Health Centre Authorities) may request to use the data and their requests will be reviewed by *"MRO-institution"* research committee which will them determine if planed usage is appropriate or not".

Section 3.0 states that the Program Manager is the custodian of data unless agreed upon in writing otherwise, and is responsible for collection, management, and retention of such data. This clause appoints the Data Protection Officer as required by the Data Protection and Privacy Act of 2019.

Section 4.1: This section outlines the protocol for data requests. Clearly defining principles of findability and accessibility of data. It states that all data requests must be made using the *"MRO-institution"* data request form. The completed form should be submitted to the research committee, which consists of the program manager, monitoring, and evaluation coordinator, among others. The research committee will review all requests within 30 days of receipt. Section 4.1 further classifies data requests as; "Limited access e.g. for presentations, publications, masters and PHD thesis, research, and Unlimited access e.g. *"MRO-institution"* internal, M&E reports (MoH, Districts, WHO, Other stakeholders, Monthly or quarterly etc)"

Section 4.1, Page 10; "The monitoring and evaluation office shall be responsible for documenting all data releases; the data release log shall be available on record; any applicant shall appeal to the *"MRO-institution"* data committee to review the restriction placed on data or review a decision to deny access to limited data".

The policy highlights the value of data and how it should be accessed and shared. The policy defines data ownership by stating that *"MRO-institution"* owns the data. Stakeholders who want to access these data need to submit a request which has to be reviewed by the *"MRO-institution"* IRB for approval. The policy establishes the Program Manager as the custodian of the data unless agreed otherwise in writing. Establishment of the custodian of the data is in tandem with the Data Protection and Privacy Act of 2019. However, the policy creates a loophole when it states that "..... unless agreed otherwise in writing." This implies that for a particular agreement, the *"MRO-institution"* risks giving the power attached to the office the data custodian (as established by law) to a third party. This may their ownership of these data, and consequently hinder access and sharing with other stakeholders as stipulated in this policy. The policy enables unlimited access in appropriate circumstances. This serves the purpose of data sharing.

2.6.2 MRO 2

This is a draft policy and references the Uganda Data Protection and Privacy Act of 2019 and the PEPFAR Data Governance Guidance 2021. MRO2 is "deeply committed to safeguarding the privacy and protecting the personal data of its individuals including clients, staff and partners." MRO2 acknowledges the importance of availing that "recognizes the importance of maintaining the confidentiality, integrity, and availability of data entrusted to us." The policy was designed to "to protect the fundamental right to privacy of individuals data/information. In an era of increasing digitalization and data collection, individuals need reassurance that their personal data is handled responsibly and with respect for their rights." It also aims to foster trust with its clients, researchers, or users. The policy highlights the need for accountability. The policy also emphasizes that data should be collected in formats acceptable to MoH such as those used in DHIS2. This enables interoperability of data.

Furthermore, MRO2 declares the desire to share data and that "An individual or organisation is free to publish the results of the data collected from research participants provided" and coauthor ship has to be agreed ahead of time. The policy delegates an officer to guide on which data can be shared.

2.7 International Policy Frameworks

International partners are major stakeholders in Uganda's healthcare system. They fund part of the health budget and fund many health research projects in the country. This closely knit and very important collaboration means that we have, in one way or the other, to look at how their laws impact data sharing across borders. At the international level, we reviewed the European Union (EU) General Data Protection Regulations and the Helsinki Declaration and the Global Data Facility.

2.7.1 The Helsinki Declaration

Under section B, subsection 13, the code asserts that "The researcher has the obligation to provide monitoring information to the committee, especially any serious adverse events." Subsection 21 maintains the need to protect the privacy of a person, "The right of research subjects to safeguard their integrity must always be respected. Every precaution should be taken to respect the privacy of the subject, the confidentiality of the patient's information and to minimize the impact of the study on the subject's physical and mental integrity and on the personality of the subject."

2.7.2 EU General Data Protection Regulations

Article 1 (4) states that, "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality." This seems to imply that the authorities may process (which may include sharing) of personal data even without the owner's consent provided it is for the good of the Union. Article 1 (5) seems to further assert this by allowing flow of personal data across borders within the Union.

Article 1 (63) gives the data subject the right to access their personal data, "A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, ..."

Article 1 (156) guides on how research data should be handled. It states that, "The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data that do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data)." It further states that, "The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

2.7.3 Global Data Facility

This is the initiative of the World Bank aimed at implementing key recommendations and insights from the World Development Report 2021: Data for Better Lives, enable the implementation of the Cape Town Global Action Plan for Sustainable Development Data, and close data gaps around the Sustainable Development Goals.

2.7.3.1 World Development Report 2021: Data for Better Lives

This report aimed to answer two fundamental questions; First, how can data better advance development objectives? Second, what kind of governance arrangements are needed to support the generation and use of data in a safe, ethical, and secure way, while also delivering value equitably? The report acknowledges that people are "central actors transforming data into useful information that can improve livelihoods and lives" and "enabling the reuse and repurposing of data is critical if data are to lead to better lives." The "potential benefits that people realize in the form of improved policies and service delivery may increase rapidly as more data, especially personal data, are shared and reused—but the risks of data being misused increase as well."

The report identifies three pathways through which data can advance development objectives, i.e., (i) the use of data by governments and international organizations to support evidence-based policy making and improved service delivery, (ii) the use of data by civil society to monitor the effects of government policies and by individuals to enable them to monitor and access public and commercial services, (iii) the use of data by private firms in the production processes to fuel their own growth as well as wider economic growth. The report further highlights the need for equity in sharing the "benefits of data when investments and regulations create a level playing field" and thus the "need for a new social contract around data—that is, an agreement among all participants in the process of creating, reusing, and sharing data that fosters trust that they will not be harmed from exchanging data and that part of the value created by data will accrue equitably." The report highlights the important role of laws and policies in ensuring resourceful sharing and reuse of data. It states that, "Legal systems, and governance more generally, can be viewed as instruments for establishing, facilitating, and enforcing social contracts.

Persuading parties to abide by the rules of a social contract is not an easy task and will hinge on ensuring that the benefits from using data are shared in an equitable way—that is, everyone has something to gain. In this process, lower-income countries are too often disadvantaged, lacking, as they often do, the infrastructure and skills to capture data and turn them into value; the institutional and regulatory frameworks to create trust in data systems; and the scale and agency to participate equitably in global data markets and their governance." Social contract here implies that there is a well-designed data governance framework that creates trust in the integrity of the data system, while ensuring that the benefits of data are shared equitably. This in turn allows the country to "capture the full economic and social value of both public intent and private intent data and leverages synergies between them." The social contract involves three main components, i) Trust: A trust environment is created when the rights and interests that all stakeholders have in data are safeguarded, ii) Equity: All share equitably in the benefits of data when investments and regulations create a level playing field, iii) The full value of data materializes when systems enable the use and reuse of data for different purposes.

Advancing development objectives through data: this can be achieved through;

i) Disseminating, exchanging, and sharing data to enhance data reuse and repurposing

ii) Unlocking data for the public good and safeguarding against misuse

iii) Public intent data can improve service delivery, targeting, accountability, and empowerment. Data can lead to better lives through three main pathways: first, by improving policy making and service delivery; second, by prioritizing scarce resources and targeting them to reach marginalized populations and areas; and third, by holding government accountable and empowering individuals to make better choices through more information and knowledge.

iv) Private intent data can fuel growth and boost development: Innovations in the use and application of data by businesses are creating tremendous economic value by enhancing data-driven decision-making and reducing transaction costs.

v) Combining and repurposing data can deepen their development impact: Combining different types of data can fill data gaps and offer new perspectives on development problems.

vi) Improving data infrastructure helps ensure equitable access for poor people in poor countries.

The report mentions the importance of aligning data governance with the social contract.

i) Improving data infrastructure helps ensure equitable access for poor people in poor countries

ii) Data laws and regulations can help create an environment of trust: Trust in data transactions can be supported through a robust legal and regulatory framework encompassing both safeguards to promote trust in data transactions by avoiding or limiting harm arising from the misuse of data, and enablers to facilitate access to and reuse of data within and among stakeholder groups to ensure that the full social and economic value of data can be captured.

iii) Aligning data regulation with economic policy objectives can support the creation of value

iv) Sound institutions and governance can improve the development impact of data: If institutions do not function well, policies and laws and regulations are unlikely to be implemented or enforced effectively, and infrastructure will not deliver on its potential. An effective institutional framework for data governance must fulfill several critical functions, such as setting policy objectives, developing supporting rules and standards, enforcing compliance with such regulations, and continually improving governance through learning and evaluation. To maximize buy-in from all participants in the data governance ecosystem, including society more broadly, data management must be socially inclusive and perceived as legitimate.

2.7.3.2 Cape Town Global Action Plan for Sustainable Development Data

The document is a plan to address gaps in national statistics and statistical coordination identified in response to the 2030 Agenda. In order to achieve this, the plan identified key principles which include accountability and cooperation among countries and organisations.

Accountability: The modern production of statistics requires comprehensive interaction among data providers, producers and users. Therefore, trust among data providers, producers and users of statistics is key for the effective functioning of the national, regional, and global statistical systems in full adherence with the UN Fundamental Principles of Official Statistics. Accordingly, the plan identifies national statistical systems, under the leadership of National Statistical Offices as the necessary and appropriate leaders of this effort.

Cooperation: The Plan recognizes the crucial role of cooperation among countries, regional organizations, and other international organizations and stakeholders in supporting countries' plans and efforts in capacity building. The Plan recognizes the expertise and abilities of these key stakeholders as essential resources for progress and modernization. Indeed, they have a crucial role in capacity building exercises and in carrying out statistical capacity building efforts in their areas of work. Nonetheless, the role of international organizations and regional entities to the development of methodologies and data in their respective programmes must be conducted in full consultation and coordination with National Statistical Offices. Coordination and streamlining of these activities are necessary to avoid duplication of efforts and channel efforts to furthering the agenda. Effective accountability builds trust among stakeholders across all levels of the data ecosystem. This is critical in ensuring effective sharing of health-related data.

3.0 Results of Key Informant Interviews

We purposefully selected key informants from a preliminary list of key actors identified from the document review. We interviewed key informants who had a role in developing and/or implementing data management and sharing policies in Uganda. A total of 23 participants were interviewed (see a description of participants in appendix 1). Analysis of the interviews showed six themes that are explained in detail below. We extracted a few excerpts to illustrate the themes. Although we present the themes individually, in practice the themes influence each other, which further exemplifies the complexity of health data sharing. The themes show the challenges that need to be addressed and the opportunities that should be leveraged for harmonious health data sharing.

3.1 Control

As identified in the document analysis of data sharing policies in Uganda, the laws do not protect the weaker entity during the contract negotiations about data control and access. Quite often, local institutions are the weaker entity and their interests in the data they collect are not protected by the current laws, and this negatively affects the findability, accessibility, interoperability, and reusability of the data.

> *'The intention was that we do not want to share our data and the institution we have shared with disappears and forget about us thinking it's their data and that they can do anything they want with it. This is something that we are struggling with some of our collaborators,' (Policy Developer).*

> *'In terms of data sharing and protection processes, one must seek approval from the Executive Director. Then from within the organisation, staff usually sign a code of conduct. We also sign demand disclosure statements and statements of confidentiality,' (Policy Implementer).*

> *'Some donors impose stricter data protection requirements. So, you need to be able to come to demonstrate compliance with those before you can even qualify for funding, but we also consider the risks to the existence of the organisation,' (Policy Developer).*

> *'So long as you are dealing with the data from your institution, there are limits to what you can share and with whom. Data sharing takes different dimensions. Funded projects such as the NIH ones have more restricted procedures for data sharing. In this case, it appears that the institutional policy may not really apply. It appears the project contract is more powerful than the institutional policy. In other instances, there's some bit of flexibility, especially if the participants were enrolled in the setting where the requester is in the same country and you're going to use data within the country, then it's usually the Principal Investigator to authorise data sharing,' (Data User).*

> *'There is software and platforms where once you upload the data, it goes to the funder directly. You cannot change anything once it has been sent. If you make a mistake, you have to send the correction to them. Similarly, in case, you want to access and reuse the data, you have to request them,' (Data User).*

Issues of control and authorisation in relation to health data sharing have significant impact on how health data is shared. The findings show that the current laws and policies are focussed on ensuring privacy at all costs, leaving little room for sharing data. This is exacerbated by inter-jurisdictional considerations, where data sharing policies of funders take precedence over policies of host institutions in Uganda. Funders outside of Uganda are expected to comply to the Data Protection & Privacy Act in the same way as local companies but they exploit the opportunity to negotiate their contracts and through that they have their policies take precedence. Even when the policies align, it is a challenge when the policies of funders

take precedence over Ugandan institutional policies as evidenced in the quotes above. These authorisation procedures prohibit equitable sharing of health data. There is a need to examine and streamline the existing administrative and authorisation procedures to balance control over data among concerned stakeholders. This will in the long run enable efficient sharing of health data.

Data sharing i.e. practice of making data available to others, is directly affected by data access i.e. the ability to retrieve and manipulate data stored in a database or other data storage systems. Data access takes several forms, including no access which is the most extreme, allowing access to data products and not the data directly such as insight reports, limited access, and lastly full access to data. The health data sensitivity-access-control dynamics is illustrated in figure 2 below. To achieve the benefits of data sharing, there must be a good balance between privacy and access to data. This can be achieved by associating adequate levels of access with consideration of the level of sensitivity rather than categorising all health data as being sensitive, while ensuring that the shared data is used for the purpose for which it was shared and primarily for common good.

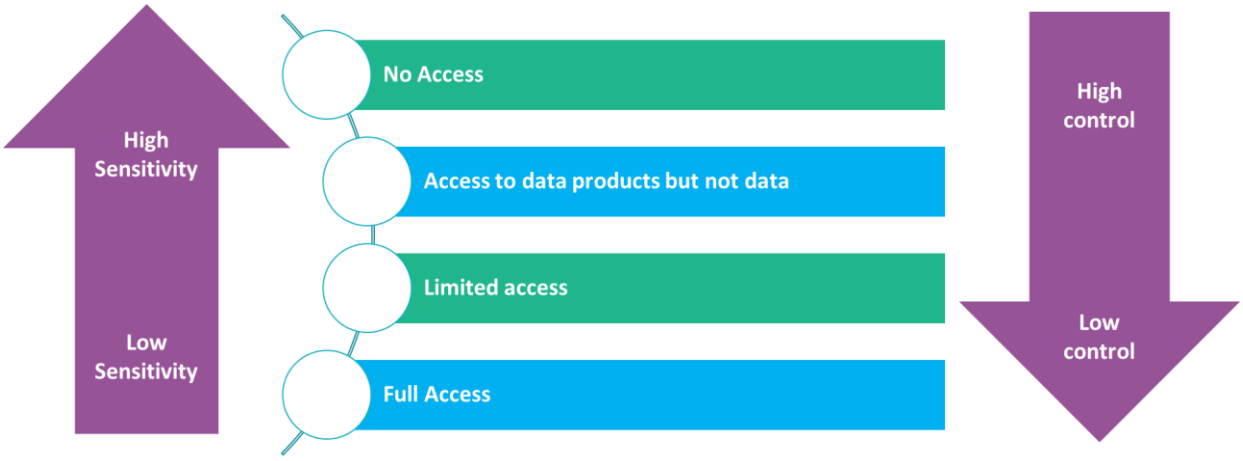


Figure 3: Illustration of the health data sensitivity-access-control dynamics

3.2 Different processes

From the interviews, we see that the procedures of accessing and sharing data differ greatly among institutions. Even in circumstances where the laws give citizens the right to access data, there are complicated procedures that often differ from what is stipulated in the laws. This highly divergent structure of procedures makes it difficult to access and integrate data from different institutions.

> *'We have a data policy and standard operating procedures managed through the information communication and technology department because that department is in charge of our servers which keep a lot of data. I am not aware of the operating procedures of data sharing, but I know that if you need data you have to request for it through the Executive Director,' (Policy Implementer).*

> *'For someone outside the organisation who want to use this data, they have to put in an application requesting through the Director of Public Health indicating the type of data they want and for what purpose. So, when we see that it's okay for example if it is for research, then we approve. We analyse for them that particular data and then give it to them,' (Policy Developer).*

'In some organisations, there are so many levels for data authorisation. There are also challenges of different people being placed to authorise data. You may find that authorisation of data is not central in some organisations. You may get access to one set of data from one authoriser and then another one needs another authoriser. The other challenge we get is that the people who are meant to authorise the use of data are not always available.,' (Policy Developer).

'We now need to put in place a data protection officer which is a new position that we have not had previously. That person will coordinate across different units because we generate different types of data so that means the restrictions to access are different,' (Policy Implementer).

'Yes, even at the Ministry level, they allow you to get this data, but you're only supposed to use it for that purpose. They analyse it from there, interpret it and leave it. They don't encourage you to pick this data from there and keep it and use it for other purposes,' (Policy Implementer).

It is difficult to access data from different organisations. It is also fair to recognise that the organisation that is the custodian of the data must take on the administrative obligation to prepare it as well as the legal risks that arise from sharing that data. Overall, the stakeholders indicated the willingness to share data. However, there was hesitancy towards sharing data due to the sensitivity and risks arising from how the data might be used or interpreted. Moreover, they indicated uncertainty about accountability for decisions based on shared data. There are efforts to harmonise data sharing procedures among local stakeholders. Some of the organisations indicated that they had good relationships at the national level, especially in terms of feeding the data they generate into the health management information system.

3.3 Centralisation

The interviews indicated that one way in which institutions implemented data sharing policies was by maintaining or depositing data into centralised data sharing systems within Uganda and overseas. Centralisation of data repositories enhances the findability, accessibility, interoperability, and reusability to facilitate sharing of data. The excerpts below highlight this point.

'The data can be accessed internally for tasks because we keep it centrally. You can easily run the query and generate information once you are given a go-ahead. We have our central systems in place to easily retrieve the data,' (Policy Implementer).

'There's an online system, a national database where we are supposed to subscribe to confirm that we have data protection systems in place. In addition to our internal systems, we also have donor preferences to reinforce what we have internally. There are data sets situated on apps from the donor data security checklist from Centres for Disease Control,' (Policy Implementer).

'As a programme, we are now gearing towards digitalization. We have introduced the pilot of smart paper technology in two of the communities using the village health teams to collect data using their phones,' (Policy Implementer).

'To strengthen data protection, we need to streamline a policy on data governance. We should have a data warehouse, a central place for data. For you to have a data warehouse, you need to automate systems because access and ease of use become much easier,' (Data Developer).

'The revisions of the e-Health Strategy seek to strengthen data sharing especially the interoperability component. We have developed registries to ensure that systems are interoperable. Now within the Ministry of Health, if you come up with an innovation, you need to bring that innovation to the technical working group within the Ministry of Health. The technical working group will look at your innovation in relation to sharing data with the master aggregator which is the DHIS. The committee will also assess the sustainability plan if the innovation is going to be piloted and use existing infrastructure in terms of human resources,' (Policy Developer).

Centralisation of data makes a significant contribution to implementing data sharing agreements among different stakeholders. Indeed, stakeholders should work with the Ministry of Health Division of Health Information by supporting the proposed health information warehouse and other existing systems. Although digitally enabled data sharing platforms facilitate timely data sharing and interoperability, there is need for stakeholders to define the ontology of the data formats and metadata requirements needed to facilitate data sharing between different digital platforms and software providers as they are increasingly being developed. This will minimise technical barriers that slow or limit data sharing within and across organisations.

3.4 Privacy, Trust, and Accountability

Data sharing and use is not a single transaction, but part of a complex data life cycle which includes data creation to collection, storage, sharing, and use. Ultimately, data sharing is an act of trust, and trust can be demonstrated through trustworthy capabilities such as technical and governance competence, robust authorisation frameworks and a clear purpose for data use.

Policy developers, implementers and users mentioned that data security and privacy such as breaches of confidentiality, commercial use and potential abuse of the data are major concerns that influence data sharing. This is a major concern among patients at risk of being stigmatised if identified by the public. It's important to realise that tightening privacy regulations makes it more difficult to access and share health data. Trust among all concerned parties is what can help establish the right balance between the desire to protect the privacy of data subjects and the need to share their health-related data.

> *'There is so much data, but it should not be easily accessible by any person because it can compromise the country's security. Even if you are doing research, you have to go through layers of scrutiny to be able to access that data,' (Policy Developer).*
>
> *'We are not allowed to share externally without the approval of senior management what I can say is that we are supposed to limit access to the database, not share it publicly,' (Policy implementer).*
>
> *'The aim of our data protection policy is first, to protect the rights of the data sources, that's why you need to keep the information with strict confidentiality. We also want to ensure that the researchers don't manipulate data in the process of doing business,' (Policy Implementer).*
>
> *'There are three principles that are vital for data sharing, respect for persons, efficiency, and justice. With respect to the people who are actually generating the data, we need to involve them in the entire process,' (Data user).*
>
> *'Data protection is important particularly now that we are talking about it, I am realizing that we have not understood the importance or the value of the data we have, and we have not put in place key things to protect it and to make sure the access to that data is regulated. Surely if you do not inform the people who are on the ground then you cannot effectively protect the data but also, we are not using the data which is interesting. We are not compiling the data, we are not looking into it, I say that as just us as an organisation and we are not using it say to inform policy. I think it is key and it is part of our mandate as people who collect this data, people who are looking at it every day to make sure that it is well protected,' (Data User).*

Developers and implementers of data policies, and data users, mentioned that accountability is the foundation of effective sharing of health data. Stakeholders should take responsibility for their data

management practices and comply with relevant regulations. Demonstrating compliance shows that an institution values privacy and is committed to protecting the data subject and their interests. This builds trust in the public and thus facilitates data sharing. The desire to foster better accountability was evidenced through purpose-driven data sharing, responsible use and re-use of data and upholding the rights of people who give the data. The findings also show that for data sharing policies to be effective, they need to be responsive to emerging strategic priorities, the different ways institutions operate, and funder requirements.

> *'People can benchmark physically to see the best practices. It gives national pride when another country asks [about best practices],' (Policy Developer).*
>
> *'The data we collect is vital for informed decision making on what vaccines or how many vaccines should be given to what kinds of people, so it's not mainly for public consumption to that extent,' (Policy Implementer).*
>
> *'To make it easier, but also beneficial for all parties involved in this process of sharing data. I think the most important part is the beneficial part because you have different points, but some people benefit immensely. Others you know a little bit here and there,' (Policy Implementer).*
>
> *'There is interference, which could be political. Much as these policies are there and the governance that protects the person who is working according to the data protection policy rules, I think it is also sometimes abused. What is lacking are the guidelines for their implementation and standard operating procedures for community usage and awareness, and then the lack of accountability clauses for people generating the data,' (Policy Implementer and Data User, Civil Society Organisation).*

It was established that data sharing policies should be value-based, purpose-driven and should be in the public's interest. Indeed, the Data Protection and Privacy Act of 2019, policies of Ministry of Health, and other relevant laws and policies emphasise that the source of data must consent for their data to be used in research or in other processes other than the primary purpose for which it was collected. The consent defines the terms and framework within which accountability will be given to the data subject. Accountability may include assurance of privacy, notification of data breaches and response, equitable sharing of the outcomes of shared data, among others. However, the extent to which the consent forms are executed regarding data use may be subject to discussion due to lack of efficient follow-up mechanisms.

3.5 Resources

There are various resources that are essential for the effective implementation of data sharing policies. Key among them are the human and financial resources as shown in the quote below. It is one thing to have policies in place and another to implement them. Human resources play a significant role in ensuring the quality, findability, accessibility, and reusability of data. Financial resources enable the recruitment of staff as well as investments in infrastructure and systems that enable data interoperable.

> *'There is a capacity gap at the local government, what they need is a diploma or certificate in record management. In terms of the structure at the Centre, there is one person, so there is understaffing,' (Policy Implementer).*
>
> *'The capacity of staff is very critical. For example, the use of DHIS2 has been limited because of the capacity of staff. The capacity to access the data from the system is also one of the limiting factors for the organization. There is a need for training,' (Data User).*

'We are supporting health systems and data collection depends on the Ministry of Health tools therefore if the tools are not available in the health facilities and in the communities, this affects the data collection and sometimes it also delays. We also rely on a digital platform to access the data which is to be determined by the internet,' (Data User).

'We need to empower people on how data should be shared or disseminated. For example, if the monitoring & evaluation manager in our organisation is sick or on leave it delays dissemination of information. We need to disseminate data sharing policies with proper guidance and mentorship to meet timeliness in terms of data quality.' (Data User).

'Not very many people are aware. So, the awareness levels are still low. The national information technology survey that was conducted in 2022 and it had sections on knowledge of the Privacy and Data Sharing Act, not particularly on the sharing but the Act and the percentages were about 33 per cent, which was definitely very low,' (Policy Developer).

"We form part of the international body which is called the International Association of Privacy Professionals. These resources enable us to keep updated with what is happening in the privacy world in data management that forms a part of expertise. The other is that we are part of associations where there are other regulators on data protection and privacy. So, there is knowledge sharing on, implementation, enforcement, best practices and these include network of African data privacy regulators, we are part of the Commonwealth resident data protection regulators that are in the Commonwealth forums, so this gives us better view and resources beyond Africa. To mention but a few those are the ones" (Data Developer).

'We need to raise awareness and I would think because now I feel more aware. To go out there and tell people who are doing research, people who are doing PhDs, and maybe it can start earlier because you start as a student and you do not understand the basics of research, you do not understand the value of data. Why do we write it in files, why do we record it in books? So, starting at that level so that as people go up the ladder they know about it. I also think that as institutions the culture needs to change. Waiting for people to come and use your data and take it and do what they want with it. If we are trained and more aware then that changes and that should be sort of an organisational thing understanding that the data we have is actually valuable,' (Data User).

Aspects of understaffing significantly compromise data sharing in many ways but notably through slowing the data sharing process or denying access because data controllers may be unavailable to give timely authorisation. Also, there may not be enough staff to facilitate the data sharing process. Furthermore, insufficient resources may negatively impact the quality of data hence rendering it unusable. Strengthening data quality processes is also key to enabling resourceful sharing of health data.

3.6 Collaboration

One of the themes that emerged directly from the interviews was the benefits of and the need for collaboration among stakeholders in the process of the development and implementation of the policies. Furthermore, collaborating on common projects fosters a conducive environment for sharing data if the collaboration is governed by fair terms. The interviewees mentioned the importance and need for collaborations among stakeholders.

'So, in other words, the COVID-19 pandemic influenced data sharing in a positive way than in a negative way because we got a lot of innovations. We also saw a growing interest in data including people we had never seemed interested in data,' (Policy Developer).

'In terms of social behaviour data from civil society, we know that they are doing a lot of work, and we are now bringing them on board. We only have maybe 20 per cent of the partners sharing data with us,' (Policy Implementer).

'The current research policy has been developed through a participatory approach [collaborative]. It is part of our institutional culture to keep updating documents with relevant information such as emerging pandemics every two years,' (Policy Implementer).

'The improvement of the policy came in gradual because the more questions the funders ask, the more improvements that you make. In developing a data policy, we aimed to have a streamlined process of managing data. We incorporated community priorities as we were developing the data protection policy because the data protection includes data at different levels even at community level. The one area which needs improvement is engaging service beneficiaries in the development of policies,' (Policy Implementer).

'The health information platforms we have developed, our clients have helped us to get data insurance around the protection to which we will be able to pursue a special risk for unforeseen implementation. So, we have tried to rely on what the client wants and how they would be able to manage the platform,' (Data User).

'The government may need to be empowered and supported to be in charge of most of these tools and software that are in place so they can be able to really regulate infrastructure,' (Data User).

Interviewees discussed the need to engage the right people at the right time from across different departments and disciplines in developing, reviewing, and implementing data health policies to ensure that they are responsive to data sharing needs. Multi-disciplinary teams are essential in bringing together the range of expertise (public health, legal, information governance, technical, policy) needed to implement health data sharing policies.

4.0 Discussion

This report highlights the extent to which data sharing issues are considered in existing laws, policies, and related working documents across different levels of governance in Uganda's health sector. The report further highlights the practices, attitudes and knowledge of policy makers, policy implementers and data users, about sharing of health-related data. These are key persons in the data eco-system that greatly impact the process of sharing the data.

The process of sharing health data among stakeholders in the Uganda's healthcare system is very complex and requires special attention. Stakeholders acknowledge the importance of sharing these data but cautioned on the need to examine the purpose of such actions to protect the data source and to maximise the benefits for common good. Indeed, the process of sharing data must protect and maintain the privacy of the data subjects. This is important for the security of these individuals, but also to avoid stigmatising patients with chronic illnesses like human immunodeficiency virus (HIV) infection, tuberculosis etc. It is therefore critical to achieve the delicate balance between confidentiality of data source as well as promoting data sharing in the interest of policy development, practice and research innovations. Thus, there is need to amend existing laws and policies so that they are up to date with prevailing needs, opportunities, and challenges regarding sharing health-related data. These laws and policies define the processes of accessing and sharing data, but more importantly define the rights of the data subjects and the obligations of all stakeholders involved in the health data eco-system. Upholding these principles will help build trust among all parties involved and thus enabling sharing of health data.

Sharing high quality data is essential for evidence-based decision making in public health sector. In Uganda, health-related data is collected by different stakeholders including MoH, local government, public and private hospitals, medical research organisations, academic institutions, and civil society. Uganda, like any other country, has a set of laws and policies at national, subnational, and institutional levels that address how data should be managed and shared. Clearly, the laws are ambiguous, and the policies differ greatly between institutions. This has led to differing procedures for accessing and sharing data at each institution thus having to deal with several complicated bureaucratic processes. If these laws and policies are harmonised, the flow of health-related data will greatly improve, and this will positively impact various health programs. For instance, during the COVID-19 pandemic, the lack of evidence to counter misinformation substantially compromised vaccine uptake in Uganda and other African countries. Insufficient sharing of data about adverse effects associated with the vaccine for example, negatively affected public perceptions on the safety of COVID-19 vaccines. We are therefore inclined to think that if health data are sufficiently shared, it enhances the information, education and communication (IEC) to the public to address concerns and counter misinformation, as well as enabling healthcare practitioners at community levels make informed decisions on vaccination and other clinical interventions. It is documented that people respond differently to medication or vaccination, and therefore consistent collection and analysis of data is crucial to advance personalised medicine, and vaccine and/or therapeutic dose optimisation and targeting. Also, data on expiry of vaccines, if shared correctly can build trust among stakeholders and the public. Keeping such data away from stakeholders hinders improvement in service delivery, and hurts trust among the public, which in turn curtails vaccine uptake.

The study has revealed that even within government itself, departments struggle to access health-related data from other departments. However, it is more difficult if the entity seeking the health-related data is external to government or to the institution holding the data. Thus, there is need for special clauses to be included in the data laws to cater for the unique requirements and challenges of data access in the healthcare system. For example, stigma is associated with misuse of clinical data, while for genomics data, the real concern is that people can be denied access to services like health insurance when the providers know about the increased risk of a particular disease like cancer in a particular individual or sub population. The timing of release of data on expiry of vaccines and other drugs may have significant impact (either positive or negative) on politics and vaccine campaigns. It is such differences that justify the need for special clauses in data laws, and robust policy frameworks to cater for health-related data. Indeed, laws and policies can ably help with these challenges by being clear on the levels of sensitivity of health-related data, defining which health-related data is deemed security sensitive and how to access and use it, who can access what type of health-related data, the procedures of data access by the different stakeholders, use and reuse of data, and how to share the benefits of the shared data. That approach will greatly enable the FAIRification of health-related data, i.e., Findability, Access, Interoperability, and responsible Reuse of vaccine data.

The constitution of Uganda is the supreme law of the land. Article 27 gives citizens the right to privacy, and this means that an individual chooses what personal data (i.e. an individual's identifiable data) can be released to third parties, with exceptions if it threatens national security, state sovereignty, and where it infringes on the right to privacy of others. This article implies that the right to privacy is not absolute. In article 41, the constitution gives citizens the right to access information held by government provided access to this the information does not compromise security. These articles apply to health data but cannot stand alone for the purposes of sharing such data. The constitution catered for this by mandating the parliament to enact additional laws to this effect. This means that parliament can be engaged to make improvements in the laws to cater for prevailing needs and challenges in the health sector.

In 2005, the parliament of Uganda enacted the Access to Information Act which detailed the type of information/data to which article 41 of the constitution applies. We deduce that information held by MoH is

directly impacted by this Act and Article 41 of the constitution since MoH is an entity of government. The Act does not exclude medical records held by government in public healthcare facilities. However, it affirms that the accessed information should not infringe on the privacy of an individual. This may mean that an individual can access medical records that have been anonymised since individuals cannot be identified if anonymisation is done efficiently. However, some forms of health data like genomics data by nature can still be exploited to narrow down to individuals who gave them. To make this clear, by using genomics data, companies like 23AndMe can be used to identify relatives of an individual and precisely locate their origins. Such situations are not well catered for in the Ugandan legal framework.

The Data Protection and Privacy Act of 2019 further clarifies on some grey areas from previous laws. This Act mainly establishes a framework for protection of personal data, and it applies to both public and private entities in Uganda. This act distinguishes between data collector (entities that collect the data), data controllers (entities that determine the purpose and means of processing personal data) and data processors (entities that process data on behalf of data controllers), elaborates their responsibilities and the rights of data subjects. In some situations, the same person or entity is the data collector, controller, and processor. This Act allows data control to be decided in data sharing agreements. However, it does not protect the weaker parties in the process of negotiating such agreements. An example here is the research collaborations where the data collector, who in majority of cases is the local institution, is the weaker party due to the many competing interests like finances and as such is unable to press for equal access (a function of data sharing) to the data they collect. This is a very complex relationship (as regards to data sharing) with complicated power dynamics.

Control over data is agreed on in contracts and agreements, which are unfortunately made in an unlevelled ground often to the detriment of the local stakeholder. This causes challenges on how local stakeholders and researchers may access, share, and use data from research projects. Consequently, this inhibits equal sharing of the benefits from these data and thus fails trust and accountability. This came out clearly in the interviews with key stakeholders where they mentioned that some funders prevent any access to the collected data leaving the local stakeholders frustrated. Also, the MoH, the custodian of the healthcare system in Uganda, in its policies left the issue of data control to the collaborating parties to decide at project inception. It is important that all stakeholders in the healthcare system realise that data subjects voluntarily give their data for defined objectives, mainly for the improvement of health for all. Their participation in studies or surveys, by law or by ethics, is not paid or induced by money or gifts. As such, funding the process of data collection does not automatically give the right of “ownership” to these data. This can be debated from various perspectives of the stakeholders, and this is why national laws and policies need to be very clear on this matter. The right to ownership, and thus access to these data should be fair and balanced among all stakeholders with the general objective of improving health for all.

The MoH is making efforts to digitise data in its custody hence facilitating easy access and sharing of these data. In Uganda, data in digital form, hence held on computers, is directly governed by the Computer Misuse Act of 2011 as amended. This Act, under section 5 (a) authorises the MoH, as the controller of the data it holds, to share these data with third parties if that data is held on a computer. In section 18 (1), the Act bars unlawful disclosure of the data if the data is to be used for any other purpose other than for which it was obtained. The definition of “purpose of obtaining data” may differ between subject and entity. To the individual going to seek health services, the data is being collected for “diagnostic/treatment purposes.” To the MoH, the entity collecting and controlling the data, the data is obtained for “diagnostic/treatment of the individual and understanding the public health dynamics in the community.” Together with the Data Protection and Privacy Act 2019, these potentially authorise the MoH to share any data in its custody with third parties provided it has been efficiently anonymised. However, none of the laws obliges the data controller to be accountable to the data subject or other stakeholders in the health data eco-system yet accountability is critical in building trust and ensuring equal sharing of the

benefits from these data. Everyone involved needs to be aware of the safeguards in place to protect the interests of all parties involved and should also share the benefits of participating in this process. This will motivate efficient sharing of health data. Furthermore, giving accountability improves communication among stakeholders, fosters a good relationship and thus enhances collaborations. Collaborations imply that entities are working towards a common goal. The current laws need to be amended to be stricter on ensuring accountability to all stakeholders and by all stakeholders.

Efficient sharing of health-related data requires robust ICT infrastructure. The MoICT is mandated to establish and maintain the national ICT infrastructure to support both public and private initiatives. The ministry has several policies and work plans aimed at achieving this objective. Indeed, there are tremendous gains in this direction. However, to maximise this potential for the benefit of the healthcare system, the MoICT must work with MoH so as to customise products that cater for the unique requirements of health-related data. The documents reviewed show that the MoH acknowledges this need and has tried to bridge with MoICT to get more precisely targeted support. However, this requires both financial and human resources if this is to be addressed. Efficient policy planning can define ways through which public and private entities can fill this gap.

The process of accessing data is marred with intense bureaucracy, even for data such as that in custody of government which by law should be readily accessible by the public. The challenges caused by immense differences in data sharing policies is exacerbated by the ambiguity and lack of clarity in the national laws that govern data, e.g., lack of clarity on the levels of data sensitivity and how they are derived, the type of data considered relevant to national security, and the circumstances under which health data can be classified as national security data. Case in point is data on vaccine adverse effects or expiry dates. Sharing these data rationally can increase trust and improve management of adverse effects thereby increasing vaccine uptake. Yet, sharing these data is highly restricted and this has a negative impact. Furthermore, results from interviews showed that requests for data are in practice submitted to the top management who are technically not the assigned information officers in public institutions and are often too busy to process such requests in a timely manner, and in some cases, may not have the expertise to appreciate the need to share the requested data. More to that, the different levels of data sensitivity are not well defined and access and sharing based on level of sensitivity is not appropriately catered for in the policies. All these put together hinder efficient sharing of health-related data.

There is need for increased investment of financial and human resources to enable advanced collection, storage, and retrieval of data, such as smart paper technology piloted by the MoH, data centres, skills development among others. This would facilitate establishment of modern infrastructure and skills which in turn will enable efficient and resourceful sharing of health data. Some institutions like Kampala Capital City Authority have invested in centralisation of data management facilities by establishing a modern data centre. The Ministry of Health is also pursuing establishment of a comprehensive data warehouse for health data. Having centralised data repositories was identified as a key factor since it would allow easy access to data and improve interoperability, but also it increases the chance of stakeholders to identify common projects on which they can collaborate. Ultimately, this will enable data to be shared more efficiently among stakeholders.

The challenges limiting efficient sharing of health-related data include the ambiguity in the laws governing data at national level such as the lack of clarity on which type of data is relevant to national security, state sovereignty and that which would be prejudicial to the person’s right to privacy, highly heterogeneous policies at institutional level, lack of sufficient resources, and the power imbalance among data subject,

data collector, data process and data controller, are major challenges. Therefore, there is a need for increased discussions among stakeholders to find solutions to these challenges.

5.0 Recommendations

The analysis identified components necessary for harmonising the legislative and regulatory framework to enable efficient sharing of health data namely, structures, processes, and people. The recommendations provide a solid foundation towards creating balance between making data accessible, safeguarding privacy, and protecting time, intellectual, and financial investments if operationalised to realise a harmonious data sharing policy framework.

- Streamlining the legal and policy framework to increase clarity on the freedoms and limitations to data access in the context of data privacy, consent, ownership, and data sharing agreements between institutions and other interested parties.
- Establishing efficient data-sharing systems and platforms that are interoperable to allow seamless sharing of health-related data among different stakeholders. Establish appropriate protocol and standard operating procedures (SOPs) to enable efficient sharing of health related data among all stakeholders. Furthermore, harmonize and clarify the responsibilities and supervision of sectoral regulators and stakeholders by establishing a data sharing governance structure that adopts a multi-stakeholder model.
- Enacting policies to guide and promote collaboration among different stakeholders, including government agencies, healthcare providers, researchers, and industry partners. This will promote the harmonisation of data sharing/access standards, protocols, and governance frameworks to meet the needs and interests of the broader healthcare ecosystem.
- Establishing robust ICT infrastructure through which data can be safely collected, stored, mined and/or shared with other parties.
- Increase financial investment and human resource in data management in both public and private institutions. ii) Establish a data sharing coordination office to coordinate data sharing across different stakeholders, iii) Include costed implementation plans to foster action, implementation, and monitoring.
- Increase public engagement and awareness about the value of data and the rights and obligations of all stakeholders including the data subjects
- It is essential to achieve a balance between privacy and data sharing. This can be achieved through efficient accountability to all stakeholders thus building trust in the entire data eco-system in the health sector.
- Health data stakeholders should consider strengthening mechanisms for evaluation, feedback and learning as part of policy implementation processes. These would provide opportunities for fine-tuning policies during implementation and could prevent well-intended policies from negatively affecting health services. Assessments of how previous policies may affect the implementation of new policies should also be considered, particularly in instances where policy objectives may have changed or be in potential conflict.
- Developing and implementing a national Health Data Strategy that considers all data management principles, legislation, rules, processes, and resources to drive policy development, practice and innovation. The process of developing this strategy should be multisectoral and involve all stakeholders in the healthcare system.

6.0 Conclusion

The legal landscape regarding data sharing and management is mixed. There is the challenge of power imbalance between data collector, data controller, and data processor. In this eco-system, data subject (data source) and data user are almost rendered powerless. This may be fixed through amending the Access to Information Act and the Data Protection and Privacy Act or if line minister passes regulations to help balance the power dynamics. There is the need for MoH to harmonise collection, storage, processing, and management of health data from both public and private facilities and institutions, and to harmonise procedures that guide data use and management in the health sector. The MoH needs to work more closely with the MoICT to develop infrastructure and tools that cater for the unique data requirements and needs in the health sector. Local governments need to be encouraged to interest themselves in developing capabilities to manage health data and to pass bylaws to this effect, since they are mandated to operate district health facilities which generate a lot of data. This will improve the flow of health data among local institutions thereby facilitating data driven decision making, in the process supporting public health initiatives like those aimed at improving vaccine uptake.

The key informant interviews with data sharing policy developers, implementers and data users provided a better understanding of key actors' views, knowledge, attitudes, and practices towards sharing health data. This study highlights the variety of factors that enable and constrain implementation of efficient sharing of health data. Most notably, it is important to build trust across the entire data eco-system. An efficient system of accountability helps build trust among stakeholders. This helps achieve a good balance between the need for privacy and sharing health data. Furthermore, it is important to establish better control mechanisms over the data, probably through decentralisation to enable timely access to the data. This issue was also evident in the review of relevant data sharing policies. Addressing these challenges will enable efficient and resourceful sharing of health-related data.

Appendix 1: Summary of the Report

Towards a Universal Health Data Sharing Policy for Uganda

A Research Summary Report

Adroit Biomedical and Bio-Entrepreneurship Research Services Limited October 2023

Benefits of sharing health data include:

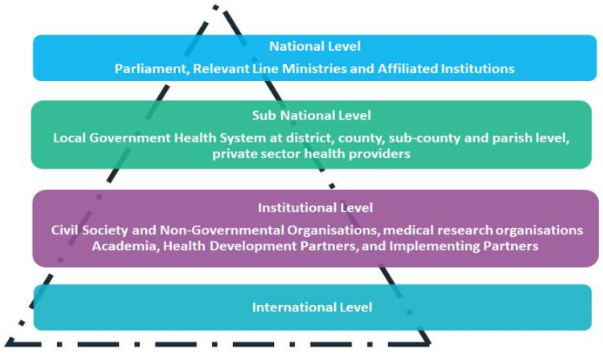
- Fostering improved service delivery, such as increasing uptake of immunization services.
- Contributing to strengthening of partnerships, which increases the chances for novel innovations to ensure good health for all e.g. new vaccines.
- Enabling fair representation of different communities and their unique medical characteristics leading to the development of medical interventions tailored to benefit all people.
- It leads to the identification of rare and geographically localised diseases and informs efficient medical interventions.

Background

Uganda has enacted laws, regulations, and policies at national, sub-national, and institutional levels that address how data should be managed and shared. Health data sharing within and across organisations supports more informed policy-making, program management, evaluation, research, and service planning, yet misalignment of these policies can be a hinderance.

We recognise that currently, vaccine data, which itself is a subset of health-related data, is governed by the general rules of data and information at national level. Access, sharing and reuse of these data is managed by institutional policies which are rooted in national laws hence inadequacies in laws at national level certainly impact data sharing processes at the lower levels.

Context of the Study

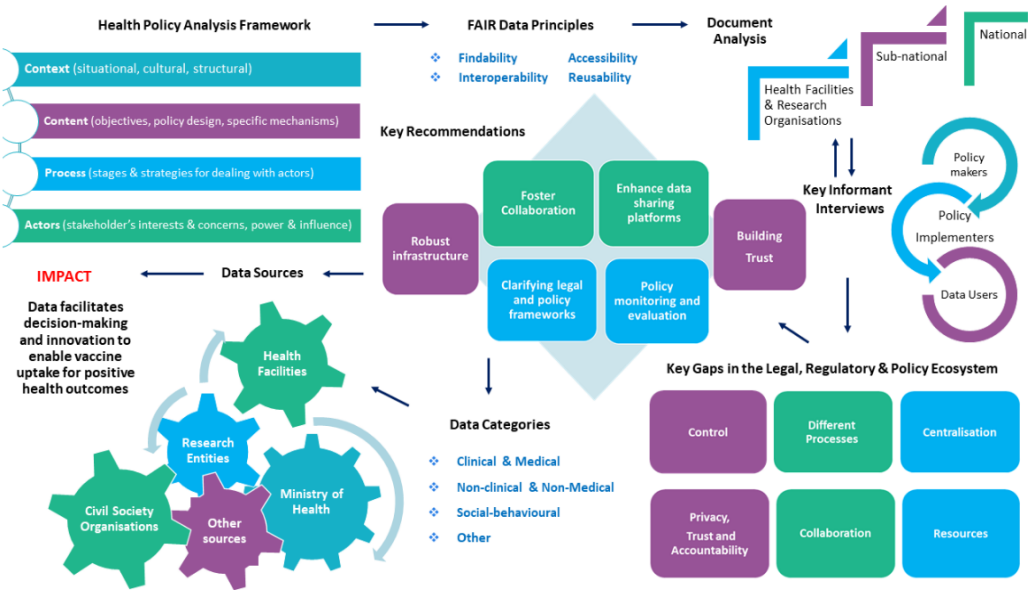


This summary report is based on extensive research that involved analysis of relevant health data-sharing policies at national, subnational, international, and institutional levels. This was followed by key informant interviews and a stakeholders meeting to validate the results.

The research aimed to identify gaps and recommendations to ensure that data laws, policies, and regulations are current, aligned and work together towards the overall goal of improving health outcomes.

The study was conducted in Kampala city.

Conceptual Framework and Methods



Gaps in the Legal, Regulatory and Policy Frameworks

The researchers investigated the data protection policies of major institutions involved in medical research in Uganda, the Ministry of Health and other relevant Government Ministries, the Constitution of Uganda, and relevant regulations and Acts of Parliament to identify gaps that prevent or hinder efficient and resourceful sharing of health-related data among stakeholders in Uganda. The key findings from this document analysis include:

Obscure Data Sharing Processes



Obscure processes of data sharing, for example, policies leave it to the collaborating parties to agree on data ownership hence the power imbalance between them may create an unfavourable outcomes for data sharing,

Ambiguious laws



Ambiguity in the laws that govern data sharing for example data holding agencies may misuse the privacy and national security clauses to deny data access to bonafide stakeholders.

Unclear definitions



Lack of clarity in the laws regarding the definition of different levels of data sensitivity, and which type of data is of interest to security organs of the state.

Various laws



Multiple laws and policies that partially address the issue of data sharing and access.

Insights from Stakeholders

These stakeholder experiences were generated from in-depth interviews with key policy developers, policy implementers, and data users such as data managers, scientists, researchers and administrators responsible for approving data sharing requests) from organisations at all levels of the healthcare system.

Control

Research respondents mentioned that it is not always clear who has control over the data and who is authorised to share it. This negatively affects data sharing.

"Some donors impose strict data protection requirements. So, you need to be able to demonstrate compliance with them before you can even qualify for funding, but we also have to consider the risks to the existence of the organisation."

Centralisation

The respondents indicated that one way in which institutions implemented data sharing policies was through maintaining or depositing data into centralised data sharing systems within Uganda and overseas.

"The data can be accessed internally for tasks because we keep it centrally. You can easily run the query and generate information once you are given a go-ahead."

Privacy, Trust and Accountability

Policy developers, implementers and users mentioned that data security and privacy such as breaches of confidentiality, commercial use and potential abuse of the data are major concerns that influence data sharing.

"There is so much data, but it should not be easily accessible by any person because it can compromise the country's security. Even if you are doing research, you have to go through layers of scrutiny to be able to access that data."

Resources

There are various resources that are essential for the effective implementation of data sharing policies. Key among them are the human and financial resources.

"We need to empower people on how data should be shared or disseminated to disseminate data sharing policies with proper guidance and mentorship to meet timeliness in terms of data quality. "

Different processes

The procedures of accessing and sharing data differ greatly among institutions. Even in circumstances where the laws give citizens the right to access data, there are complicated procedures that often differ from what is stipulated in the laws.

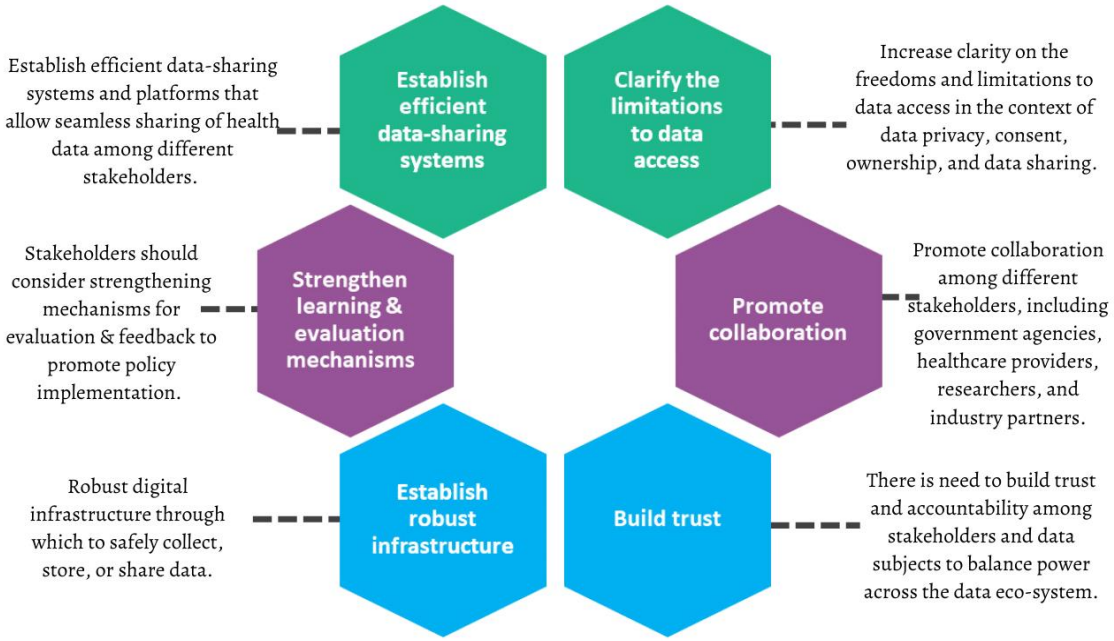
I am not aware of the operating procedures of data sharing, but I know that if you need data you have to request for it through the Executive Director

Collaboration

There is need for collaboration among stakeholders in the process of the development and implementation of the policies. Collaborating on common projects fosters a conducive environment for sharing data if the collaboration is governed by fair terms.

"In terms of social behaviour data from civil society, we know that they are doing a lot of work, and we are now bringing them on board. We only have maybe 20 per cent of the partners sharing data with us."

Key Recommendations



The recommendations provide a strong foundation towards creating balance between making data accessible, safeguarding privacy, protecting time, intellectual, and financial investments. If operationalised, these recommendations will strengthen the data sharing policy framework in Uganda.

Conclusion

This study highlights the variety of factors that enable or constrain implementation of efficient sharing of health data. Most notably, it is vital to collaborate across the entire data eco-system. An efficient system of accountability helps to build trust among stakeholders. This helps achieve a good balance between the need for privacy and sharing health data. It is important to establish better control mechanisms over the data, probably through decentralisation to enable timely access to the data.

Adroit Biomedical and Bio-Entrepreneurship Research Services Limited (ABBRS) is a not-for-profit organisation. ABBRS aims to improve health services and infrastructure through building capacity, applying modern technologies, research, and development. Our mission is to reduce the inequality in biomedicine by collaborating with people of all walks of life to advance innovations and policies that benefit all people, especially those in vulnerable settings.

The authors would like to extend warm thanks to all the respondents who contributed insights and views, and to DT Global for funding the report Towards a Universal Health Data Sharing Policy for Uganda: A Policy Analysis Report.

ABBRS

P. O. Box 112139 Kampala,
Naguru-Kampala
Email: grants@abbrs-uganda.org