

**REPUBLIC OF UGANDA
MINISTRY OF HEALTH**

THE UGANDA HEALTH DATA ACCESS, SHARING AND USE GUIDELINES

SEPTEMBER 2023

DOCUMENT REVIEWS AND APPROVALS

Version	Owner	Author	Approver	Date of Approval <i>(MMDDYY)</i>
01	Ministry of Health	Division of Health Information Management	Top Management Committee	18.09.2024

Table of Contents

Foreword	iv
Preface	v
Acknowledgement	vi
Abbreviations	vii
Definition Of Terms	viii
1.0 Introduction	1
2.0 Rationale	2
3.0 Purpose	2
4.0 Overall Objective	2
4.1 Specific Objectives	3
5.0 Development Methodology	3
6.0 Target Audience and Applicability	3
7.0 Scope of the Guideline	4
8.0 Classifying Data to Facilitate Data Access, Sharing, and Use	5
8.1 Classification Framework	6
9.0 Governance Structure	7
9.1 Roles and Responsibilities	8
10.0 Data Ownership	10
11.0 Procedures for Accessing, Sharing and Using Individual-level/Personal Data	11
11.1 Procedures for Accessing Data from Ministry of Health Data Repository	13
11.2 Procedures for Research-Generated Health Information	13
11.3 Conducting Research or any Population-Based Survey on Health	14
11.4 Data Access, Sharing and Use in Public Health Emergencies	14
11.5 Secure and Ethical Cross-Border Data Transfers	15
12. 0 Data Management	16
12.1 Measures for Confidentiality and Protection in Data Sharing	18
12.2 Data use and sharing agreement	20
12.3 Contents of the Agreement	20
13.0 Compliance and Guidelines Governance	22
13.1 Non-Compliance and Repercussions with these Guidelines	22

13.2 Liability, Penalties and Remedies	22
13.3 Sale of Health Data	23
14.0 Dissemination and Adoption of the Guidelines	23
15.0 Conclusion	23
Appendix 1: Generic Data Access, Sharing, and Use Agreement Template	26
Appendix 2: Health Data Access, Sharing, and Use Compliance Checklist	39

Foreword

The Government of Uganda promotes the use of data for decision-making and policy formulation. The Ministry of Health Strategic Plan 2020/21 – 2024/25 also recognises the use of data as a key enabler for supporting the health system to deliver good health to the population. This is further articulated in the Uganda Health Information and Digital Health Strategic Plan 2020/21-2024/25.

The Uganda Health Data Access, Sharing and Use Guidelines are intended to standardize the implementation of health data access, sharing and use across Uganda's health system. The guidelines are aligned with the Data Protection and Privacy Act 2019 to ensure the operationalisation of the law within the health sector.

These guidelines will serve as a framework to ensure secure information access, exchange, and use as well as timely identification and addressing of vulnerabilities.

In addition, the guidelines will ensure that health data is accessible while protecting the Privacy and Confidentiality of those from whom data was obtained. These guidelines shall apply to all the health practitioners both in the public and private sectors while collecting, processing, archiving, accessing and sharing data. All stakeholders in the health spectrum are therefore called upon to embrace the use of these guidelines while handling any form of the health-related data.



.....

Dr. Henry G. Mwebesa

DIRECTOR GENERAL HEALTH SERVICES


Preface

This document presents Uganda's Health Data Access, Sharing and Use Guidelines for the Health Sector. The guidelines are aligned with the Data Protection and Privacy Act 2019, Data Protection and Privacy Regulations 2021, National ICT Policy 2018, Health Information and Digital Health Strategic Plan 2020/2021-2024-2025, and Ministry of Health Strategic Plan 2020/2021-2024-2025.

Health Information and supporting systems are critical assets for health service delivery. In Uganda like in many places, health data is faced with many privacy and confidentiality threats from a wide range of sources. Therefore, protecting the health data of Uganda's health system clients is of prime importance to the Ministry of Health. These guidelines provide comprehensive guidance to healthcare providers, policymakers, and stakeholders on best practices for sharing and using health data throughout its lifecycle.

By adhering to these guidelines, we not only fulfil our ethical and legal obligations to safeguard patient privacy but also foster trust and confidence among individuals accessing healthcare services. Furthermore, these guidelines will pave the way for innovation and collaboration in leveraging health data to improve healthcare delivery, research, and public health interventions.

All stakeholders in the health spectrum are therefore called upon to adopt the use of these guidelines while handling health-related data.



.....

Dr. Sarah Byakika

Commissioner Health Services

Department of Planning, Financing and Policy

Acknowledgement

The Ministry of Health expresses its profound gratitude to all departments and programs, members of the Health Information Innovation and Research Technical Working Group and the Data Management Subcommittee who contributed technical inputs leading to the successful completion of this document. Special appreciation goes to the Division of Health Information Management (DHIM) and the Information Communication Technology (ICT) Section for the overall guidance to ensure that the guidelines are aligned with the Health Information and Digital Health Strategic Plan 2020/21-2024/25.

I acknowledge and thank all development and implementing partners that provided financial and technical support for this process, specifically MUSPH/METS, HISP Uganda, IDI and the Centers for Disease Control and Prevention (CDC). DHIM is grateful for all the support, sacrifice and contribution that has been invested in its successful development.

Finally, the Ministry of Health is grateful to the Ministry of Information Communication Technology and National Guidance, National Information Technology Authority Uganda (NITA-U), Personal Data Protection Office, National Identification & Registration Authority, Uganda Health Informatics Association, Makerere University Health Informatics Research Group, and all those institutions and individuals who have not been specifically mentioned above, but who directly or indirectly contributed to the successful development and finalization of these guidelines.

.....

Mr. Paul Mbaka

Assistant Commissioner Health Services

Health Information Management

Abbreviations

DPIA	Data Protection Impact Audit
DUA	Data Use Agreement
GRO	Grievance Redressal Officer
HIE	Health Information Exchange
HIS	Health Information System
HISP	Health Information System Programs
ICT	Information and Communications Technology
IPR	Intellectual Property Rights
MoH	Ministry of Health
PII	Personal Identifiable Information

Definition Of Terms

Anonymization	Is an irreversible process of removing or transforming personally identifiable information (PII) to a form in which a data subject cannot be identified through any means reasonably likely to be used to identify such data subject.
Biometric Data	Personal data resulting from measurements and calculations relating to the physical, physiological, or behavioural characteristics of a natural person that allow or confirm the unique identification of that natural person, such as facial images or fingerprint data.
Confidentiality	The obligations of those who receive data and/or information to respect the privacy interests of those to whom the data relates.
Consent	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
Consent Artefact	A readable document that specifies the parameters and scope of data sharing and access that a data subject consents to in any personal data sharing transaction.
Data	Data refers to raw, unorganized facts or observations that are collected, stored, and processed to create meaningful information. Data can be in the form of text, images, numbers, audio, video
Data Collector	Person or an entity that collects data.

Data Controller	A natural or legal person (e.g., an organisation or other entity) who alone, jointly with other persons or in common with other persons or as a statutory duty determines the purpose for and the manner in which data is processed or is to be processed.
Data Processor	Person/entity other than an employee of the data controller that processes data on behalf of the data controller.
Data Protection Officer	Is an individual employed by a data controller who understands and applies data protection regulations to the data control operations and serves as a liaison between the data controller and regulators.
Data Subject	is an individual from whom or in respect of whom personal information has been requested, collected, collated, processed, or stored.
De-identification	The process by which a data controller or data processor may remove or mask identifiers from personal data, or replace them with a fictitious name or code that is unique to a data subject but does not, on its own, directly identify the data subject.
Disclosure	Refers to the act of revealing or making information known, often in a formal or public context for transparency, accountability, or legal compliance.

Data Sharing	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.
Data Access	Data access refers to the function of providing access to the shared data to the correct entities.
Encryption	The process of transforming data/value into code to prevent unauthorized access.
Health Data	Personal data related to the physical or mental health of a natural person, including the provision of health care services that reveal information about their health status.
Natural Person	Any person with rights and responsibilities defined by international human rights conventions
Notification	A legally defined process of informing about an intention to access and use personal data
Personal Data	Any information about a person from which the person can be identified and/or includes an expression of opinion about the individual.
Personal Health Identifier	A subset of “personal data”, is the data that could alone or combined with other information potentially identify a data subject and/or be used to distinguish one data subject from another; a personal health identifier could also be used to re-identify

	previously de-identified data and could include a data subject's demographic and location information, family and relationship information, and contact details.
Personally Identifiable Information	Any data that can be used to identify an individual. Personally identifiable information includes but is not limited to names, physical and internet protocol addresses, financial information, login information, biometric identifiers, video footage, geographic location data, social media accounts, email addresses, and insurance identification numbers.
Privacy	An individual's right to control the acquisition, use, or disclosure of their personal information.
Processing	Any operation performed on personal data, such as collecting, creating, recording, structuring, organizing, storing, retrieving, accessing, using, seeing, sharing, communicating, disclosing, altering, adapting, updating, combining, erasing, destroying, or deleting personal data; or restricting access or changes to personal data; or preventing destruction of the data.
Protection	Refers to the practices, policies, and measures implemented to safeguard and manage the privacy, integrity, and confidentiality of personal and sensitive information.
Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately so as to ensure that the personal data is not attributed to an identified or identifiable natural person.

Sensitive Data	This means that the stored data have confidential and/or personal data, therefore, processing such data is limited.
Sensitive Personal data	Refers to information that, if disclosed, could result in harm to individuals or organizations.
Third-party	A natural or legal person, public authority, agency, or body other than the data subject, data controller, or data processor, and a person who, under the direct authority of the data controller or data processor, is authorized to process personal data.

1.0 Introduction

The world has experienced exponential growth in the demand for access to health-related data, spurred by the recognition of its pivotal role in driving innovation and enhancing service delivery across healthcare systems. This heightened demand has been further fueled by rapid advancements in Information Communication Technologies (ICTs), which offer unprecedented opportunities to augment and optimize initiatives aimed at harnessing health data for various purposes.

Data sharing is an important way to increase the ability of researchers, academia, scientists and policy-makers to analyze and translate data into meaningful reports, knowledge and informed decision-making. Currently, health data analytics activities require fetching, integrating and/or triangulating data from different sources using rigorous scientific techniques and advanced technologies. Indeed, the ultimate goal of doing these tasks is to generate evidence that crosses national and sub-national lines. Most importantly, timely data sharing, with recognition of the interests of investigators and respective institutions who collect the data, is essential for expedited translation of research results into health policy to improve national and subnational health programs in Uganda.

In Uganda, the generation and use of data for evidence-informed decision-making have been the health sector's priority for a long time. The Ministry of Health (MoH) has been implementing the Health Information and Digital Strategic Plan with the objective of maximizing the availability, accessibility, quality, and use of information for decision-making processes. To enable data access, sharing, and use, the national adoption of key technical standards is needed. This guideline has adopted the Uganda Health Information Exchange and Interoperability Guidelines, the Uganda Health Data Protection, Privacy, and Confidentiality Guidelines, the Data Protection and Privacy Regulations 2020, the Data Protection and Privacy Act 2019, The National Information Security Policy (framework) 2014, The National Records and Archives Act 2001 and The Access to Information Act (2005)

2.0 Rationale

The landscape of health data management in Uganda faces significant challenges due to the absence of comprehensive standards for data access, sharing, and use. The lack of these standards at all levels of the health system leads to suboptimal utilization of data, breach of personal privacy and confidentiality, and misunderstanding of data ownership. In light of these challenges, formulating data access, sharing, and use guidelines is essential to address gaps, enhance data utilization, and ultimately improve health outcomes across Uganda.

3.0 Purpose

The guidelines seek to establish an effective, transparent, and accountable framework for managing health data access, use and sharing in Uganda.

By establishing these guidelines, several important aspects will be addressed:

- a) Maximizing health data use for decision-making
- b) Improving health data transparency and accountability
- c) Minimizing duplication of efforts
- d) Clarifying ownership of health data and information
- e) Foster a collaborative approach to health data management
- f) Improving individual health data privacy, confidentiality, and security
- g) Facilitate collaboration among researchers, policymakers, and healthcare practitioners, fostering a conducive environment for health research.

4.0 Overall Objective

The overall objective of this guideline is to define a set of principles, requirements, strategies and procedures that guide health and health-related data sources or owners to enhance data access, sharing and use within and between the institutions and individuals who own and/or deal with health and health-related data.

4.1 Specific Objectives

- a. Promote and ensure the health administrative units and health facilities, research institutes, academia, agencies, researchers and development partners share health data and evidence as openly as possible;
- b. Facilitate clear and transparent health data access and sharing practices using standard procedures among relevant stakeholders
- c. Define procedures for health-related data classifications for better data access and sharing practice;
- d. Define the roles and responsibilities of health data owners, controllers and users during data storage, access and sharing processes

5.0 Development Methodology

A consultative approach was used in the development of the guidelines. Stakeholders from the Ministry of Health (MoH), Ministry of ICT and National Guidance, Personal Data Protection Office (PDPO), Ministry of Public Service, NITA-U, NIRA, Development and Implementing partners, Civil Society Organizations, Academia, and other members of the Health Information Innovation and Research (HIIRE) Technical Working Group (TWG) collaborated in developing these guidelines.

6.0 Target Audience and Applicability

These guidelines are intended for both the public and private sector targeting a wide range of stakeholders involved in the data management within Uganda's health ecosystem. This includes:

- a. General Public
- b. Healthcare Providers: Clinicians, nurses, and other healthcare professionals responsible for collecting and managing health data.
- c. Data Managers: Personnel responsible for organizing, storing, and maintaining health data within health facilities and institutions.
- d. Policymakers: Individuals involved in developing health policies and strategies at national, regional, and local levels.

- e. Researchers: Scientists and researchers conducting studies using health data for epidemiological, clinical, or public health research.
- f. Technical Personnel: IT specialists and developers involved in designing and implementing health information systems.

7.0 Scope of the Guideline

These guidelines typically cover issues like data ownership, intellectual property rights, permitted uses of the data, data security, and data sharing duration. The scope of this guideline are as follows:

Covers the access, use and sharing of data only, excluding biological samples

- a. Covers the access, use and sharing of health data in the context of the Public and Private Sector i.e. Ministry of Health services and programs.
- b. Provides a mechanism to share other health data than those already being collected, processed, anonymized, analyzed, and shared.
- c. The guideline will not be applied retrospectively to data sharing agreements already in place, except where the same is being renewed or there are amendments to such data sharing agreements.
- d. Data access is governed by the data processing obligations listed in the Uganda Health Data Privacy, and Confidentiality guideline.

8.0 Classifying Data to Facilitate Data Access, Sharing, and Use

Data classification by data sources/owners is one of the first steps in moving towards a data-sharing paradigm. Data elements are classified based on the sensitivity and impact of the sharing of that data to the users. Data held by data sources can be of the following types.

Sn	Sensitivity Level	Classification and Dissemination Methods	Data and Information Types
1	<p>Low Sensitivity Data elements with minimal risk or impact if accessed or disclosed.</p>	<p>Classification: Public Data This type of data is freely accessible to the public. It can be freely used, reused, and redistributed without repercussions.</p>	<ul style="list-style-type: none"> ● Aggregate outline/institution-based health information data. ● Surveys and surveillances ● Program-specific evaluations ● Approved reports and published documents.
2	<p>Moderate Sensitivity Data elements containing identifiable or sensitive health information requiring protection.</p>	<p>Classification: Internal-only Data Data that is strictly accessible to internal organizational personnel or internal employees who are granted access.</p>	<ul style="list-style-type: none"> ● Ongoing/unpublished research works/papers (manuscripts) ● unpublished/ unendorsed or non-finalized works e.g. Textual/print documents, audio, video, images, graphical or cartographical materials), ● Biological specimen with no unique identifier (to prevent uncontrolled depletion) ● Uniquely identified data of routine and survey data
3	<p>High Sensitivity Data elements with significant privacy or security implications, requiring stringent safeguards and access controls.</p>	<p>Classification: Confidential Data Access to confidential data requires specific authorization and/or clearance. This may contain identifiable or sensitive health information requiring protection.</p>	<ul style="list-style-type: none"> ● Biologic specimen with unique identifier ● Aggregated survey results (e.g. aggregated to the household level and with additional disaggregation based on different indicators)

			<ul style="list-style-type: none"> ● Registries for health workers, clients and health products ● Financial statements and accounts.
4	<p>Severe Sensitivity Information or data that, if disclosed or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede the conduct of the work of a response.</p>	<p>Classification: Restricted Data Restricted data includes data that, if compromised or accessed without authorization, could lead to criminal charges and massive legal fines or cause irreparable damage to the organisation. This may have significant privacy or security implications, requiring stringent safeguards and access controls.</p>	<ul style="list-style-type: none"> ● Physical/recorded or biologic data of individuals with unique identifiers. ● Geographic position data of military health facilities linked to military bases and training facilities. ● Raw survey data, e.g. individual survey responses at HH-level data ● Personal data of beneficiaries (i.e. Beneficiary lists, patient records, etc.) ● Line lists/line listing data

8.1 Classification Framework

To effectively classify health data, organizations should adopt a structured approach:

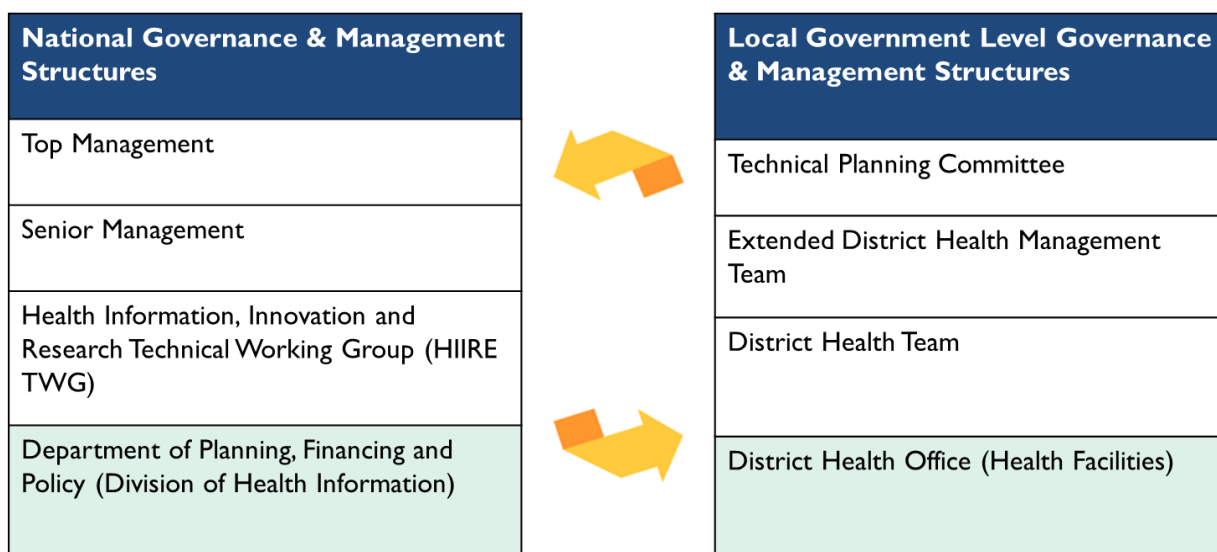
1. **Data Inventory:** Catalog all types of health data collected and processed by the organization.
2. **Sensitivity Assessment:** Evaluate the sensitivity and risk associated with each type of health data.
3. **Access Controls:** Implement access controls based on data sensitivity to limit who can view and process the data.
4. **Policy Implementation:** Develop and enforce policies and procedures for handling, protecting, and sharing health data.
5. **Regular Review and Update:** Periodically review and update data classifications to reflect new types of health data and changing regulatory requirements.

9.0 Governance Structure

The Governance of health data access, sharing and use shall follow the existing governance and management structures at the national and decentralized levels, as summarized in Figure 1.

Technical oversight is the mandate of the Division of Health Information Management (DHIM) under the Department of Planning, Financing and Policy which guides and coordinates all stakeholders involved in health data collection, processing, use and storage. This function is similarly decentralized at the Local Government level, as summarized in Figure 1.

The main task of the Health Information Innovation and Research Technical Working Group (HIIRE TWG) is reviewing and giving advice on Health Information Systems (HIS) and Data and Digital Health policy and strategic related issues from the user departments and other stakeholders.



The Ministry of Health together with the Personal Data Protection Office (PDPO) shall be responsible for monitoring the application of these Guidelines in order to protect the fundamental rights and freedoms of natural persons in relation to collection, processing, storage, access, sharing, and use of their personal data and to facilitate the free flow of personal data within and outside the country in relation to health service delivery.

The PDPO shall represent the supervisory authority in any dispute or conflict arising from infringement of the provisions of these Guidelines.

At the national and subnational levels, a Data Protection Officer (DPO) shall in addition to the functions identified under these Guidelines, communicate with regulators and external stakeholders on matters concerning data privacy and serve as an escalation point for decision-making on health data governance and other matters concerning health data.

The roles and responsibilities of the data controller, data processor, and Ethics and Data Sharing Coordination Committee are described below;

9.1 Roles and Responsibilities

1. Data Controller

The controller at the national level shall be the Director General of the Ministry of Health; at District/City level, the District Health Officer/City Health Officer shall be the data controller for all public and private health facilities in the district; and at the facility level, the data controller shall be the Health Facility In charge.

- a. The data controller shall implement appropriate technical and administrative measures to ensure data access, sharing and use are performed in accordance with these guidelines and other related guidelines.
- b. The controller shall consider the nature, scope, context, and purposes of data collection, processing and confidentiality risks at varying likelihood and severity of impact on the rights and freedoms of data subjects, and this shall determine technical and administrative measures to be put in place.
- c. Upon receiving a request for data, the data controller shall consider the intent and extent of data processes, which have varying likelihood and severity of risks to natural persons. The controller shall determine the means of collection, data processing, and he or she will also implement appropriate technical and administrative measures, such as pseudonymization and minimization, including other integral safeguards that meet the requirements of these guidelines to share and use data securely.

- d. The controller shall implement appropriate technical and administrative measures (including physical measures) to ensure that, upon receipt of a request for access and data sharing, the following are taken into consideration:
 - i. That a data sharing agreement (*Sample Template in Appendix 1*) is duly reviewed and approved.
 - ii. Ensure that the data sharing agreement clearly stipulates the type of personal data collected, the extent of their processing, the period of their storage, and their accessibility
 - iii. Only personal data that are necessary for each specific purpose shall be processed
 - iv. Ensure that consent is provided before access to personal data of a natural person is provided.
 - v. Ensure adherence to the Data Protection and Privacy Act 2019.
- e. In the event of any personal data breach, the Data Protection, Privacy, and Confidentiality Guidelines shall be followed to guide what is to be done in case of a data breach. This will include reporting all data breaches to the Personal Data Protection Office immediately after becoming aware of it.

2. Data Processor

- a. The primary role of a data processor is to process data according to the instructions provided by the data controller or as defined in a data processing agreement (*Template provided in the Uganda Health Data Protection, Privacy and Confidentiality Guidelines*). This may involve tasks such as data collection, recording, structuring, storage, retrieval, modification, use, transmission, and erasure.
- b. The processor shall not reassign the role to another processor without prior specific or general written authorization of the controller.
- c. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
- d. Processing shall be governed by the approved data processing agreement, that shall clearly stipulate the subject matter, and duration of the processing, the nature and purpose of the

processing, the type of personal data, the categories of data subjects, and the obligations and rights of the controller.

- e. When a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in a data processing agreement or other legal contract between the controller and the processor shall be imposed on that other processor by way of a data processing agreement or other legal contract under the Uganda Data Protection and Privacy Act 2019. Should that other processor fail to fulfill his or her data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.
- f. The data processing agreement or other legal contracts shall be in writing, including in electronic form.

3. Ethics and Data Sharing Coordination Committee

The role of the Ethics and Data Sharing Coordination Committee is to oversee the ethical aspects of collecting, storing, processing, and sharing health data for scientific research and healthcare service delivery. This committee reviews and approves such activities to ensure they comply with ethical standards. Even when data processing meets legal requirements, controllers and processors must implement safeguards to mitigate ethical risks. These risks include processing individuals' health data who haven't consented, using techniques that infringe upon data subject rights, and sharing data with entities outside the country.

The other roles and responsibilities of the data collector and the data protection officer are further described in **Section 8** of The Uganda Health Data Protection, Privacy and Confidentiality Guidelines.

10.0 Data Ownership

Data ownership shall remain the property of the research institute, agency, department, ministry, health facility, health system clients or any entity that generated/collected it in line with established norms.

Institutions shall develop data management and sharing plans at the proposal stage. These plans shall outline the strategies for collecting, managing, storing, accessing, sharing and use research data throughout the research project lifecycle. Approval from relevant approval bodies shall be obtained before the commencement of the research, ensuring that data-sharing practices align with ethical and legal standards.

Significant portion of health-related research/surveys is funded by private and foreign institutions, these funders shall require researchers to make their data available in national databases and repositories for reuse. Institutions engaged in health-related surveys/research shall establish and maintain up-to-date data-sharing plans. These institutional plans shall outline the procedures and protocols for collecting, storing, accessing, sharing, and use of research/survey data.

11.0 Procedures for Accessing, Sharing and Using Individual-level/Personal Data

- 1) Any health worker or health institution that suspects or comes across epidemic-prone diseases that are regarded as reportable by health authorities shall immediately notify the concerned authorities.
- 2) All relevant institutions shall timely notify/report vital events information that are regarded as reportable by relevant health bodies.
- 3) Any holder of individual-level data has the responsibility to prevent illegal use, unauthorized access, data loss and modification.
- 4) Only individuals with a role and responsibility assigned to them by the health institution shall have access to individual-level data and shall have access to the data only for the purpose of care of the individual.
- 5) Any one owning individual-level data shall maintain privacy, and confidentiality and shall not share the data to any entity unless permitted by or in compliance with a specific law of the country.
- 6) Any health service recipient has the right to access or obtain his/her information stored in the health facility, which renders him/her health care.

- 7) The usage, sharing and publicizing individual-level data is only permissible for the health care of the individual and other aims permitted by the law of the country.
- 8) Unless by order of a court or required by the health professionals' ethics committee, the original copy of the individual-level record shall not be taken out of the health institution. If the data is kept or has backup in digital format or Electronic Medical Record (EMR), it is permissible to consent with the individual, in a de-identified manner and generally in a manner, which doesn't put the confidentiality of the data at stake.
- 9) Individual-level data shall be stored in a secured place, which does not allow entry to and access to data other than authorized individuals.
- 10) If a particular health facility is closed out, handed over or closed down, the data under its custody shall be transferred to a health facility which has replaced it or to the health administrative unit which has been overseeing it or has been reporting to.
- 11) The holder of individual data can share and permit its use apart from the purpose of health care to the individual if consent is obtained from the individual in writing and the purpose is properly stated.
- 12) Any data owner/source can share individual-level personal data with a third party or permit its use without the consent of the service recipient/individual under the following conditions:
 - a. When sharing the data and use by a third party is required by legal enforcement bodies, or when the law requires it;
 - b. Sharing the data to next of kin or caregiver of the individual in the interest of care of the individual and if an individual is not in a state or condition to consent;
 - c. When the use or sharing of the data to a third party is necessary to prevent the public or the individual from any harm;
 - d. When the use of the data or sharing with a third party is essential for the purpose of refunding from health insurance schemes;
 - e. When required by the health care provider regulators and for court purposes and when ordered by the appropriate court and regulatory bodies;
 - f. The use or sharing/disclosure of the data is deemed essential for public health.

11.1 Procedures for Accessing Data from the Ministry of Health Data Repository

To obtain data from the Ministry of Health data repository, the following steps shall be followed

Step 1: First, a formal data sharing/access request shall be submitted to the Ministry of Health's Director General's (DG) Office in writing, and the DG shall forward the request to the Assistant Commissioner of Health Services ACHS, Division of Health Information Management (DHIM).

Step 2: ACHS DHIM shall inform data requesters to submit detailed data-sharing requests by filling out the MoH's data request form. Then the ACHS DHIM shall evaluate the data request in accordance with the MoH's eligibility for data sharing/access and other relevant criteria and advise the DG accordingly.

Step 4: The DG shall approve or reject the data access/sharing request. Once the data request has been approved, the data sharing agreement template shall be filled out, signed, and stamped by the two parties (DG's Office and the data requesting institution/person.)

In case the data request is rejected, the data requester shall be duly notified within a reasonable time frame usually within five working days.

Step 5: An officially delegated individual will be authorized to access data based on the objectives of the data request. The ACHS DHIM shall be responsible for the overall data governance, and management and shall be accountable to the Director General. The DHIM unit will be responsible for the overall management of the national health and health-related data.

11.2 Procedures for Research-Generated Health Information

Research on health is conducted by individuals, institutions or organizations. It is intended to influence policy formulation, introduce new approaches to treatment or health management and to prove or disprove a hypothesis but all in all, to generally lead to betterment in health care. Efforts to utilize research findings have been minimal. Researchers conduct their research and there is nobody to encourage the use of the findings. For example, findings of research done as part of fulfilment of a PhD or Master's degree, are hardly used because they are not disseminated and the researchers do not know how to share this information.

11.3 Conducting Research or any Population-Based Survey on Health

Step 1: The researcher(s) shall write to the Uganda National Council for Science and Technology (UNCST), copied to the Uganda National Health Research Organization (UNHRO) of the Ministry of Health, indicating the following:

1. Study to be done
2. Reasons for conducting the study
3. Intended beneficiaries of the study
4. The geographical area that the study will cover
5. In case biological samples are to be taken, this shall be stated and the specific samples (blood, urine, spinal fluid, etc) and the study subjects indicated
6. Duration of the study

Step 2: Submission to the appropriate Institutional Review Board (IRB) shall be done.

Step 3: Following IRB approval, the researcher shall submit to the National Council for Science and Technology, the institution shall use its criteria to determine whether to give the authority or not.

Step 4: The National Council for Science and Technology shall give the response to the researcher(s) in writing, copied to the Uganda National Health Research Organization (UNHRO).

11.4 Data Access, Sharing and Use in Public Health Emergencies

During public health emergencies, such as pandemics or outbreaks, data access, sharing and use guidelines become even more critical to ensure effective response efforts while safeguarding individual rights and privacy. These are the procedures to be followed in Uganda.

- a) Access to relevant health data during public health emergencies shall be facilitated promptly to support timely decision-making and response efforts.
- b) Authorized government agencies, public health institutions, and designated healthcare providers shall have expedited access to necessary data for surveillance, monitoring, and epidemiological investigations.
- c) Access requests shall undergo streamlined review processes to minimize delays while ensuring compliance with ethical and legal standards.
- d) Data collected during public health emergencies shall be used solely for purposes related to outbreak detection, response planning, and intervention implementation.
- e) Healthcare providers and public health officials shall adhere to established protocols and guidelines governing the use of emergency health data.
- f) Data use shall be guided by principles of necessity, proportionality, and respect for individual privacy rights.
- g) Measures shall be in place to ensure the accuracy, integrity, and confidentiality of data used for decision-making and policy formulation during emergencies.
- h) Mechanisms for secure data sharing shall be established to facilitate real-time exchange of information while protecting sensitive data from unauthorized access or disclosure.
- i) Data sharing agreements shall be in place to define the scope, purpose, and limitations of shared data, as well as to address issues related to data ownership, intellectual property rights, and confidentiality.

11.5 Secure and Ethical Cross-Border Data Transfers

When data needs to leave Uganda and be transferred to another country, additional guidance and precautions shall be implemented to ensure the security, integrity, and ethical handling of the data. Observe the following for such data transfers:

- 1) Shall conduct a thorough analysis of the legal and regulatory requirements in both the originating and receiving countries. Uganda's data transfer requests shall be in accordance with the Data Protection and Privacy Act 2019.
- 2) Ensure adherence to other national and international laws, treaties, and agreements governing cross-border data transfers.
- 3) Obtain necessary approvals from relevant regulatory bodies before initiating data transfers outside the country.
- 4) Data Sharing Agreements (DSAs) shall be signed between the originating and receiving countries.
- 5) Respect for personal or individual autonomy and rights of individuals.
- 6) Shall utilize secure data transfer methods like secure file transfer protocols (SFTP) and virtual private networks (VPNs) for data transmission.

12. 0 Data Management

This section provides a comprehensive overview of the utilization, analysis, publication, release, and retention/destruction of shared data.

The Ministry of Health, partners, and researchers will develop data management plans that encompass the following components:

- a. **Data Description:** This element describes the following:
 - i. Information to be gathered; for example, PII or non-PII.
 - ii. Nature of the data (i.e., whether sensitive or restricted).
 - iii. Scope, which defines the data elements that are accessible in a subset of tasks.
 - iv. Scale, which is a description of measurements of the data to be produced.
- b. **Existing Data Sets:** A common guide on how to assess existing data sets for purposes of clarity and determining whether the current data sets are adequate for gathering information about program indicators.

- c. **Formats:** Specifications of "authorised or acceptable" formats to ensure processing, sharing, storage, and retrieval are more efficient Reference must be made in this plan to other guidelines on interoperability and security.
- d. **Description and Standards of Metadata:** An in-depth description of data by means of elaborating on the method of creation, standards used, purpose, time and date of creation, and authorship.
- e. **Storage and Backup:** A detailed description of how and where copies of data files will be stored to ensure confidentiality and safety. Further guidance on data storage shall be obtained from **Section 5.5** of The Uganda Health Data Protection, Privacy and Confidentiality Guidelines.
- f. **Roles and Responsibilities Matrix:** A section of the data management plan elaborates on the roles and responsibilities of data controllers, data collectors, data processors, and data protection officers in the different stages of the data life cycle.
- g. **Intellectual Property Rights (IPR) and data co-ownership:** A common agreement on which parties hold IPR to the data and other information created or collected and how to obtain permission to use or disseminate data.
- h. **Archiving Selection and Retention Period:** A description of how the data will be selected for archiving, how long the data will be stored, and plans for the eventual transition or termination of data sharing in the future. Data retention, archival and disposal shall follow **Section 5.6** of The Uganda Health Data Protection, Privacy and Confidentiality Guidelines.
- i. **Archiving and Preservation:** An outline of the procedures in place or envisioned for long-term archiving and preservation of the data, including succession plans for the data.
- j. **Ethics and Privacy:** Provisions on how an informed consent process will be carried out while ensuring that personal information remains confidential and is only made available for secondary analysis as stipulated by legal processes. Managing of consent under this section shall follow the Consent Framework detailed in **Section 10** of The Uganda Health Data Protection, Privacy and Confidentiality Guidelines.
- k. **Data Breach Management:** Non-compliance will be handled using the channels outlined under the governance structure. Personal data breach and incident management shall follow **Section 13.2** of The Uganda Health Data Protection, Privacy and Confidentiality Guidelines. The designated Data Protection Officer (DPO) and the Grievance Redressal

Officer (GRO) shall undertake monitoring compliance functions, and any matters concerning dispute resolution shall be channeled through the supervisory authority.

12.1 Measures for Confidentiality and Protection in Data Sharing

The steps that will be taken to ensure the confidentiality and protection of shared data are:

a. Technical standards

In electronic data exchange, modern technologies that promote an integrated, open, and flexible digital health solution will be used. The choice of exchange/data sharing system shall be guided by fundamental elements in relation to its ability to integrate, its cost-effectiveness, sustainability, and the ease of use of infrastructure components. Technical standards shall follow Section 2 of the Uganda Health Information Exchange and Interoperability Guidelines.

b. Confidentiality and security

To protect the privacy and security of health data, the following minimum requirements shall be implemented

- i. **Data anonymization:** Organizations and projects shall consider putting in place procedures to explore alternatives for using PII before sharing; for example, coding data, replacing original names or values with non-identifiable data, or removing unnecessary variables that may indicate individuals.
- ii. **Protect electronic transmission:** Procedures to protect data transiting between systems/persons shall be password protected and encrypted, and a receipt acknowledgement mechanism shall be implemented. The communication and connectivity protocols shall follow **Section 2.2** of The Uganda Health Information Exchange and Interoperability Guidelines.
- iii. **Data release procedures and purposes:** Provisions for protecting PII when releasing data shall be in line with data sharing principles and compliance with national and international jurisdictional laws and policies. The applicable principles are:

1. Data of public health importance shall be openly shared subject to respecting appropriately established restrictions and in accordance with international standards of ethical research conduct.
2. Sharable public health data will remain available within a minimum agreed time delay at a favorable cost, if any, for all users in support of equity to access.
3. Individuals who produce, share, and use data are stewards of the data and have the responsibility for ensuring authenticity and preserving the quality and integrity of the data, including respect for data sources, through maintenance of confidentiality/privacy by ensuring appropriate citation and acknowledgment of the original work and data repository.
4. Where necessary, data shall be labeled “sensitive” or “restricted” following proper justification and within clearly defined procedures. In any event, should sensitive or restrictive data be made available, it shall be on the least restrictive basis possible.

iv. **Data release procedures—Recipient**

Procedures for recipient individuals or partner organizations to protect PII shall be carried out under defined conditions stated as follows:

1. Have the recipient sign a confidentiality agreement.
2. Ask the recipient for documentation on security procedures, such as training, assessments, internal governance structures, and procedures for electronic and physical security controls.
3. Request the recipient to comply with the agreement to destroy information after the purpose of the data release has been fulfilled.
4. Confirm verification/evidence of access to the bare minimum amount of data and time needed to satisfy the purpose.

v. **Disposition of electronic-based information**

Provisions to securely dispose of information after the expiration of the minimum agreed period shall be put in place. This can be achieved by doing the following:

1. Eliminating e-mails sent or received containing PII
2. Sanitizing or destroying hard drives or mobile devices (including USB keys) that contain PII before the computers/mobile devices are reassigned to non-program staff members, sent offsite for repair, sold, or disposed of
3. Keeping records of documents destroyed
4. Asking partnering organizations to action items [i–ii] above

Overall, the disposal of health data shall follow **Section 5.6** of The Uganda Health Data Protection, Privacy and Confidentiality Guidelines.

12.2 Data use and sharing agreement

A data-sharing agreement is a formal contract that documents the data being shared and how the data can be used. Such an agreement serves two purposes. First, it protects the entity providing the data and ensures it will not be misused. Second, it prevents miscommunication on the part of the provider of the data and the entity receiving the data by ensuring that any questions about data use are discussed. Before any data are shared, the provider and data requester shall discuss data sharing and data use issues and develop a collaborative understanding that will be documented in an agreement. **Appendix I** provides a template that is customizable for institutions and agencies in need of sharing data under a legally binding framework.

12.3 Contents of the Agreement

The agreement between MoH and the party interested in accessing data must at least comprise but not be limited to the following components:

1. **Period of agreement** that clearly defines when the data controller will give the data or samples to the data requester how long the data requester will be able to use the material and what will happen to the data afterwards (i.e., deleted, destroyed, or returned).
2. **Intended use** of the data that states as specifically as possible how the data requester will use the data, including the studies that will be performed, questions that will be asked, and the expected outcomes. In addition, this section of the agreement shall

address whether or not the data requester can use the data to explore additional research questions without the provider's approval.

3. **Constraints on the use** of the data, which lists any restrictions on how the data/Biological Specimens or findings can be used, including whether or not the data requester is required to document how the data are used if the data requester can share, publish, or disseminate data/biological specimen findings and reports without prior approval from data controller, if the data requester can share, sell, or distribute data findings on any part of the database, and if the data requester publishes a report based on the data who the report will belong to.
4. **Data confidentiality** which describes the required processes that the data requester must use to ensure that data remains confidential. Because some data may contain information that can be linked to individuals, it is important to put safeguards in place to ensure that sensitive information remains private. Personal information shall remain confidential and not be disclosed verbally or in writing to an unauthorized third party by accident or otherwise.
5. **Data security** which describes the methods that the data requester must use to maintain data security. Hard copies of data shall be kept in a locked cabinet or room, and electronic copies shall be password-protected or kept on a secure disk. Biological Specimens shall be kept in a secure location protected from unauthorized persons. This section will note who at the data requester agency will have access to the data, how it will be protected, and what will happen to the data at the end of the sharing period.
6. **Methods of data sharing** that identify the way in which data will be transferred from the provider to the data requester (i.e., physically or electronically, encrypted or not).
7. **Financial costs** of data sharing, which clarifies who will cover the monetary costs of sharing the data. This may include transportation or postal costs.
8. **Termination of agreement** - If one of the agreements will not be fulfilled by the data requester, MoH has the full right to terminate the agreement with/without notice within 2 weeks.

13.0 Compliance and Guidelines Governance

1. The DPO of the PDPO together with the DPO of the Ministry of Health shall ensure adherence to these Guidelines and shall be responsible for compliance with all Uganda applicable laws in force.
2. All individuals and entities who are covered by these Guidelines must comply with its requirements and, where requested, demonstrate such compliance.
3. The compliance checklist developed (**Appendix II**) shall be used for the purpose of monitoring the compliance of stakeholders to these guidelines.
4. These Guidelines may be revised from time to time. A copy of these Guidelines together with any significant revisions shall be made publicly available through the Ministry of Health official communication channels like e-Library or the Knowledge Management Portal.

13.1 Non-Compliance and Repercussions with These Guidelines

Non-compliance with these guidelines may have several adverse consequences, including:

1. **Compromised Data Integrity:** Failure to adhere to data management standards may result in inaccuracies and inconsistencies in health data, undermining its reliability and usability.
2. **Breach of Confidentiality:** Improper handling of health data may lead to breaches of confidentiality and privacy, violating individuals' rights and confidentiality regulations.
3. **Ineffective Data Sharing:** Lack of adherence to standardized data sharing protocols may impede collaboration and data exchange efforts, hindering informed decision-making and research.
4. **Legal Ramifications:** Non-compliance with relevant legislation and regulations governing health data management may result in legal sanctions and penalties within the laws of Uganda.
5. Where any person or entity to whom these Guidelines is applicable is found to be in violation of any of its provisions, such a person or entity may not be permitted to participate in the national health care enterprise and further action shall be taken by the PDPO.

13.2 Liability, Penalties and Remedies

Shall follow the Data Protection and Privacy Act 2019 and any other relevant laws concerning penalties (e.g., administrative, financial, criminal) liabilities and judicial remedies.

13.3 Sale of Health Data

Sale or offer to sell health data by a person or an entity shall be prohibited. **Section 37** of the Data Protection and Privacy Act 2019 shall be followed in case of non-compliance.

14.0 Dissemination and Adoption of the Guidelines

The Uganda Health Data Access, Sharing and Use Guidelines shall be disseminated for adoption.

The dissemination and adoption of these guidelines shall happen at national, sub-national and community levels as guided by the MoH. Some of these methods are;

- a. Presentation of the guidelines to stakeholders at all levels.
- b. Posting of the guidelines on the Ministry of Health websites, WhatsApp groups, Radio etc for access by the stakeholders.
- c. Organising quarterly workshops to sensitise stakeholders

15.0 Conclusion

Ensuring adoption and adherence to The Uganda Health Data Access, Sharing, and Use guidelines in a country requires a multi-faceted approach that combines education and training, research collaboration, enforcement, and monitoring. Here are some proposed effective strategies to encourage adoption and adherence to consider for inclusion in the guideline:

1. **Stakeholder Engagement and Collaboration:** Engage stakeholders from various sectors, including government agencies, healthcare providers, researchers, patient advocacy groups, and technology vendors. Involve them in the development of guidelines to foster a sense of ownership and collective responsibility. Regularly communicate and collaborate with stakeholders to address concerns, gather feedback, and ensure their active participation in implementing the guidelines.
2. **Education and Training:** Provide comprehensive education and training programs to all stakeholders, including healthcare professionals, researchers, data custodians, and administrators. Train them on the importance of health data access, sharing, and use, as well as the guidelines and policies in place. Offer ongoing training

opportunities to keep them informed about emerging best practices, legal requirements, and technological advancements.

3. **Clear communication and awareness campaigns:** Develop clear and accessible communication channels to disseminate information about the guidelines, their purpose, and their benefits. Launch awareness campaigns targeting healthcare professionals, patients, and the general public to increase understanding and promote a culture of responsible data access and sharing. Use various mediums, such as websites, newsletters, seminars, and social media, to reach a wide audience.
4. **Incentives and Recognition:** Offer incentives and recognition programs to motivate and reward individuals and organizations that demonstrate exemplary adherence to the guidelines. This can include public recognition, awards, funding opportunities, or access to exclusive resources. Incentives can encourage compliance and promote a positive environment for health data access, sharing, and use.
5. **Enforcement and Accountability:** Establish mechanisms to enforce compliance with the guidelines. This can involve conducting regular audits, assessments, and inspections to ensure adherence to data governance policies. Implement sanctions or penalties for non-compliance, such as fines, loss of privileges, or reputational consequences. Transparently communicate the consequences of non-compliance to deter violations and reinforce accountability.
6. **Technical Solutions and Infrastructure:** Develop or enhance technical solutions and infrastructure to facilitate secure health data access, sharing, and use. This can include implementing robust data security measures, standardized data formats, interoperability frameworks, and secure data-sharing platforms. Provide healthcare providers and researchers with user-friendly tools and technologies that comply with the guidelines and streamline data management processes.
7. **Monitoring and Evaluation:** Continuously monitor and evaluate the implementation of the guidelines to assess their effectiveness and identify areas for improvement. Collect feedback from stakeholders, conduct surveys, and analyze data to measure the level of adoption, identify challenges, and address gaps.

Regularly review and update the guidelines based on lessons learned and emerging trends.

8. **International Collaboration and Benchmarking:** Collaborate with other countries and international organizations to share best practices, and lessons learned, and benchmark against global standards. Learn from successful implementations in other jurisdictions and adapt relevant strategies to the local context. Engage in international discussions and initiatives to align guidelines with evolving global norms.

By combining these strategies, the country can promote a culture of adherence to The Health Data Access, Sharing, and Use Guidelines. It requires a holistic approach that addresses education, communication, incentives, enforcement, technological infrastructure, and ongoing evaluation to ensure sustained adoption and compliance.

Appendix 1: Generic Data Access, Sharing, and Use Agreement Template

[insert name of the department/unit]

DATA ACCESS, SHARING, AND USE AGREEMENT

For [insert study title and timeframe]

Background and Purpose

This Data Access, Sharing, and Use Agreement (“Agreement”) is entered into between the [insert name of the department/unit], by and through its [insert sub-unit name, if any] and [insert name of the proprietor of the data] (also referred to herein as “Participating Entity”), individually referred to as “party” and collectively referred to as the “parties”. This Agreement establishes the basic terms and conditions for the sharing, protection, and use of certain data as defined within the context of [insert survey name] supported by [insert formal name of protocol]. The [insert name of the department/unit] may release data to entities and partners with an approved Data Use Agreement (DUA) for purposes authorized by the Participating Entity. All persons with data access must sign this agreement outlining the terms and conditions for using the data. It also sets forth the expectations for each party’s roles and responsibilities in this regard. Through this Agreement, the Participating Entity authorizes [insert sub-unit name] to use, store, process, and maintain the above-referenced data within the specified system as defined below and sets forth the expectations for each party’s roles and responsibilities. A DUA is specific to the individual project, and all projects require annual review by [insert name of the department/unit] and a designated representative from the Participating Entity.

The [insert name of the department/unit] conducts a detailed review of every application for access to data and makes a determination on a case-by-case basis. Requests for confidential (identifiable) data will be granted only if the project meets the criteria, a valid rationale for the project not using de-identified information is provided, and final approval from the Participating Entity is obtained.

Approved applicants has to complete the data requestor information form (Table 1) and are held to the highest ethical standards and must agree to the stipulations detailed in this DUA.

Authorities

The [insert name of the department/unit] is authorized by the [insert the name of the act/law authorizing the department/unit] to maintain active surveillance of diseases through epidemiologic and laboratory investigations and data collection, analysis, and distribution and to participate with other countries in cooperative endeavours related to certain health care–related activities.

The Uganda Data Protection and Privacy Act 2019 governs the collection of health care, surveillance, historical, statistical, and research data to prevent or mitigate a serious and imminent threat to public health, public safety, or the life of the data subject or another individual. In addition, the Policy/Act provides protections as required by Uganda’s law around transferring such data outside of Uganda.

Table 1: Data Requestor Information

Name	
Title	
Organization / Center / Division / Agency / Affiliation	
Mailing address	
Telephone number (including country code)	
Email address	
Contact person (if different from requestor)	
Contact person's telephone number (if different from requestor)	
Contact person's email address (if different from requestor)	
Does this application update a previous Data Use Agreement?	<ul style="list-style-type: none"> • Yes • No • Not applicable

Description of Parties and Key Points of Contact

The focus, scope, and goals of the data sharing set forth in this Agreement are aligned with efforts of the [insert name of the department/unit] and the Participating Entity for data use and access for the [insert data types] in Uganda. Accordingly, the parties, systems, and points of contact are provided below.

The Participating Entity in Uganda represents and warrants that it has the authority to enter into this Agreement as contemplated by this Agreement and that doing so will not violate any law or regulation applicable to the Participating Entity in Uganda or any agreement or arrangement to which the Participating Entity in Uganda is a party.

Each party will identify an individual to serve as the focal point to coordinate communication and activities related to sharing [insert data types] data and the coordination of the terms of this Agreement. Appendix A lists the named individuals designated as Key Points of Contact for performance of the terms of this Agreement. As part of this Agreement, both parties agree to notify each other within five (5) days when a change in Key Points of Contact occurs.

Project title	
Purpose of project	
Brief description of project (e.g., background, rationale, objectives, and methods)	
Duration of project	<ul style="list-style-type: none"> • 0–3 months • 4–6 months • 7–9 months • 10–12 months • ≥13 months
<p>Is data custodian* for project same as requester?</p> <p>If no, please indicate the name of the data custodian and their relationship to the requestor’s organization.</p>	<ul style="list-style-type: none"> • Yes • No (explain)

* The data custodian is responsible for observance of all conditions of use and for establishment and maintenance of physical and electronic security arrangements to prevent unauthorized use. This individual must have the legal authority to keep the information confidential and maintain confidentiality. If the custodian is changed, the organization must promptly notify the [insert name of the department/unit] and the Participating Entity within five (5) days of change.

Supporting Documentation for Data Access	
<p>Is release letter or letter of support from the participating entity attached?</p> <p>If no, please explain why not.</p>	<ul style="list-style-type: none"> • Yes • No (explain)
<p>Is release letter or letter of support from another agency or partner needed?</p> <p>If yes, is letter attached?</p>	<ul style="list-style-type: none"> • Yes • No • Not applicable • Yes

	<ul style="list-style-type: none"> • No
<p>Has project been approved by the appropriate Human Subjects Review Board(s) (e.g., Institutional Review Board)?</p> <p>If yes, please provide documentation and details of review and approval.</p> <p>If no, please explain why not.</p>	<ul style="list-style-type: none"> • Yes (explain) • No (explain)

Data Files Requesting and Specifications

File name	
Format	<ul style="list-style-type: none"> • CSV • SAS • Excel • Other—please specify: • Access
Timeframe for data file requested (e.g., data range in month/day/year format)	
Geographic area for data file requested	
Variables requested	
If requesting confidential (non-anonymized, not de-identified, sensitive) data, please provide a few sentences of a rational for needing these data.	

File name	
Format	<ul style="list-style-type: none"> • CSV • SAS • Excel • Other—please specify: • Access
Timeframe for data file requested (e.g., data range in month/day/year format)	
Geographic area for data file requested	

Variables requested	
If requesting confidential (non-anonymized, not de-identified, sensitive) data, please provide a few sentences of a rational for needing these data.	
File name	
Format	<ul style="list-style-type: none"> • CSV • Excel • Access • SAS • Other—please specify:
Timeframe for data file requested (e.g., data range in month/day/year format)	
Geographic area for data file requested	
Variables requested	
If requesting confidential (non-anonymized, not de-identified, sensitive) data, please provide a few sentences of a rational for needing these data.	

Terms of Agreement

Generally, the parties will adhere to a shared vision for maintaining the integrity of the [insert data types] and respecting that proprietorship of the information remains with the Participating Entity in Uganda.

The following outlines the necessary activities, roles, and responsibilities to ensure the successful management and availability of [insert data types].

Data

No data processed, stored by, or submitted to [insert name of the department/unit] for that purpose under this Agreement by the Participating Entity in Uganda will include personally identifiable information (PII) (e.g., participant names, addresses, etc.) unless all parties agree to release PII.

MAKE NOTE OF EXCEPTIONS

Consent

As per the survey protocol under which the information was originally gathered, [insert name of the department/unit] accepts data submitted by the Participating Entity in Uganda with the understanding that all individual participants have agreed to participate in the source survey and, as such, have provided their informed, voluntary consent consistent with applicable laws, regulations, and policies.

IF DIRECTLY COLLECTING, WILL NEED TO DEVELOP CONSENT FORM IN LINE WITH COUNTRY'S DATA PROTECTION ACT

Data Submission

As technology and connectivity vary, [insert name of the department/unit] will collaborate with the Participating Entity in Uganda to determine the best approach for the secure transfer of [insert data types]. It is anticipated that a technology such as that provided by [insert name of the department/unit]'s secure file transfer protocol or similar service will be utilized. [Insert name of the department/unit] will work with the Participating Entity prior to data transfer to determine specific protocols, credentials, and transmission requirements/alternatives. In no case will [insert name of the department/unit] accept data via insecure transfer methods, as defined by [insert name of the department/unit], including, but not limited to Dropbox, Google Drive, or email. Consistent with the laws of Uganda, _____ will accept responsibility for the security of the information provided only after it has been received via the agreed-upon method.

Data Quality, Error Notification, and Correction

[Insert name of the department/unit] will use its best efforts to provide feedback within a reasonable period to the Participating Entity in Uganda to resolve identified data incompleteness, inaccuracies, and inconsistencies. The Participating Entity in Uganda will research and resolve the issues and provide corrections and clarifications to [insert name of the department/unit] through the processes defined under Data Submission. Also, should the Participating Entity proactively identify any errors or have concerns about the data in use, they are asked to contact the [insert name of the department/unit] programmatic point of contact for the relevant survey and data steward/owner as defined in Appendix A.

Data Security, Storage, and Transmission

[Insert name of the department/unit] shall establish appropriate administrative, technical, procedural, and physical safeguards in accordance with Uganda's data protection act; e.g., Republic of Uganda No. 4 of 2019: Data Protection and Privacy Act], [insert name of the department/unit] security policies, and the [insert name of the national standard-setting authority, e.g., National Institute of Standards and Technology] Risk Management Framework, including formal System Security Authorization for any data or health information system that [insert name of the department/unit] creates in Uganda. Once data is received and accepted by [insert name of the department/unit] using the submission process outlined above, [insert name of the department/unit] accepts responsibility for the secure storage, transmission, and use of the information as outlined herein to the extent required by the laws of Uganda. Except as required by the laws of Uganda and as set forth in this Agreement, data submitted by the Participating Entity in Uganda residing in the [insert name of the department/unit] data system will not be physically removed or transmitted outside the established system security boundary without first obtaining prior written approval from the Participating Entity in Uganda. Any such approval must include the scope, purpose, and protections specific to the removal action.

Data Use

The following additional terms and uses apply to [insert name of the department/unit] under the terms of this Agreement:

1. [Insert name of the department/unit]’s use includes the right to translate the [insert data types] into any language.
2. Except as required by the laws of Uganda and as set forth in this Agreement, the [insert name of the department/unit] will not share with or export to other centers and offices within or organizations external to [insert name of the department/unit] any data without the express written permission of the Participating Entity.
3. Except as required by the laws of Uganda and as set forth in this Agreement, [insert name of the department/unit] will not release any data and/or results to the public domain without prior written agreement from the Participating Entity.
4. As part of accessing and using [insert data types], [insert name of the department/unit] may develop reports and analyses focused on the [insert response type] in Uganda. [Insert name of the department/unit] may invite collaborators and co-authors from other centers and offices within [insert name of the department/unit] and the participating entities to design, analyze, and co-author such reports and analyses. Also, [insert name of the department/unit] will share developed reports and analyses with the Participating Entity for comment before publication.
5. Except as may be required by the laws of Uganda, and as set forth in this Agreement, [insert name of the department/unit] agrees it will not present any findings or analyses arising from the use of the submitted data in any public forum, or prepare or submit such findings or analyses for publication, without first providing any such findings or analyses to the Participating Entity that provided the data on which these findings or analyses are based for such Participating Entity’s review to ensure that the findings or analyses do not contain any confidential or proprietary information.
6. To the extent any analyses, reports, or publications are developed using data submitted by the participating entity, [insert name of the department/unit] will acknowledge the contribution of data by the Participating Entity in Uganda.
7. To the extent required by the laws of Uganda and consistent with this Agreement, [insert name of the department/unit] will use all reasonable efforts to maintain the confidentiality, integrity, and ensure the security of the [insert data types] within the parameters defined herein. However, there shall be no obligation of confidentiality where: (i) the information is publicly available, or becomes publicly available, other than by action or omission of the receiving party; or (ii) the information was already known to the receiving party (as evidenced by its written records) prior to its receipt; or (iii) the information was received from a third party not in breach of an obligation of confidentiality owed to the other party.

<p>Will the study results be used for publication and/or presentation?</p> <p>If yes, please provide publication and presentation information and intended timing of this information.</p>	<ul style="list-style-type: none"> • Yes (explain) • No • Not applicable
<p>Have at least two co-authors / collaborators from the [insert name of Participating Entity] been identified and notified of this project?</p>	<ul style="list-style-type: none"> • Yes

If no, please explain why not.	<ul style="list-style-type: none"> • No (explain)
<p>Is the requested data needed for work being performed under contract / grant / cooperative agreement with the [insert name of the department/unit]?</p> <p>If yes, please provide the contract / grant / cooperative agreement number and point of contact information.</p>	<ul style="list-style-type: none"> • Yes (explain) • No • Not applicable

Data Security and Confidentiality

The release of information that may lead to the identification of individuals or be traced back to an individual record is prohibited. However, statistical and research results based on the data provided by the [insert name of the department/unit] and the Participating Entity pursuant to this DUA may be released. Any person(s) who access, disclose, or use confidential data in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

Only the listed data custodian or authorized users listed on this Agreement may access data.

Describe where data will be stored and how data will be accessed by authorized users (e.g., stored in a locked filing cabinet, password protected, residing on a physically secure server, zipped [compressed], 256-bit encrypted, on a cloud system, on an encrypted external hard drive).

Data Access Use by Others

Except as may be required by the laws of Uganda, and as set forth in this Agreement, access to data submitted by the Participating Entity in Uganda in conjunction with the Participating Entity shall be restricted to authorized [insert name of the department/unit] employees and contractors who require such access in order to perform their duties in accordance with the uses of the information as authorized in this Agreement. Such personnel shall be advised of (1) the confidential nature of the information, (2) safeguards required to protect the information, and (3) any administrative, civil, and criminal penalties for noncompliance contained in applicable laws of Uganda

The parties signing this agreement assert that they are fully aware of the policies for handling confidential (non-anonymized, sensitive) data and agree to protect these data in accordance with these policies. The parties agree not to share any confidential data with any person or other [insert name of the department/unit] employee/contractor unless that person has co-signed this Agreement.

The parties signing this Agreement agree to use the requested data files solely for the project described above and agree to the above-listed data access conditions and storage requirements. The parties also agree that any information or aggregate data derived from confidential data to be disseminated or published must be reviewed by the designated person(s) within the [insert name of the department/unit] or the Participating Entity. Data will only be disseminated and published in aggregate, summary form so no one individual is identified from the data. The parties also agree that they will not disclose or publish any results based on the data without a review and approval from the [insert name of the department/unit] and the Participating Entity.

Please identify the individuals who will have access to or be using the data, describe their role and work they will perform in the project, and have them sign the DUA.

Your signature below says that you have read and agree to comply with the terms of this DUA as well as with the provisions set out on this form. It is your responsibility as a user of the data to protect the confidentiality of the data and to prevent unauthorized use of or access to it.

Requester name	
Signature	Date
Printed name	
signature	Date
Description / role in project	
Printed name	
signature	Date
Description/role in project	
Printed name	

Signature		Date
Description / role in project		
Printed name		
Signature		Date
Description / role in project		
Printed name		
Signature		Date
Description / role in project		

Data Destruction

Consistent with Uganda laws, applicants must make provisions for the destruction of records at the conclusion of their project, or when the data are no longer required. Maintaining the privacy of the individuals whose personal information is included in the data is required to preserve the integrity of the data sharing process.

Data that have been shared with the [insert name of the department/unit] consistent with this agreement will be archived, stored, protected, or disposed of in accordance with relevant Uganda requirements. In the event the [insert data types] reach the end of their active lifecycle, they will be retired in compliance with formal system retirement, data destruction, and records management requirements in accordance with Uganda law, agency policy, applicable System Security Authorization, and [insert name of the national standard authority]. All data not retained as per Uganda management requirements will be destroyed using [insert name of designated authority; e.g., Ministry of Information Communication Technology and National Guidance]–authorized physical and/or electronic methods applicable to sensitive information.

Upon written request and to the extent possible, a copy of all [insert data types] will be created and returned to the Participating Entity prior to the above removal. The specifics (e.g., media, format, transport method) of this action will be determined by joint agreement between the parties when/if

needed, but must minimally comply with all relevant [insert name of the department/unit] information security and records management controls.

Please detail below the manner and timeline for data destruction according to requesting agency's / institution's / organization's policies. If following a data destruction policy set by the requesting agency / institution / organization, please attach that policy to this DUA.

Privacy Questions and Incident Response

Should the Participating Entity in Uganda have [insert data types] privacy-related questions, the need to request privacy or security-related information, or the need to notify [insert name of the department/unit], the data steward, or Ministry of Health with privacy and security-related concerns or a potential identified data breach, the Participating Entity should contact the [insert name of the department/unit] Point of Contact as provided by [insert name of the department/unit] protocol. If necessary, general inquiries may also be made to the Points of Contact listed in Appendix A.

In the event of a suspected incident (e.g., loss, theft, compromise) affecting the security of data provided by the Participating Entity in Uganda, the [insert name of the department/unit] director will ensure that formal notice is provided to [insert name of the department/unit] Cybersecurity Program Office and the Participating Entity within one (1) hour of event identification. Cybersecurity Program Office personnel, with full assistance from the [insert name of the department/unit] team, will then follow the established agency process for formal incident investigation, remediation, response, and communication as appropriate to all affected parties.

Agreement Term and Termination

This Agreement takes effect upon its signature by both parties and does not have a predefined end date but may be terminated by either party with sixty (60) days advance written notice to the other party.

The rights and obligations of the parties as set forth in this Agreement that are intended by their nature to survive its expiration or earlier termination shall survive indefinitely. This includes, but is expressly not limited to, the obligations of security, confidentiality, and usage of submitted data by [insert name of the department/unit].

This Agreement sets forth the entire agreement of the parties with respect to the subject matter hereof. In the event that any portion of this Agreement is held to be invalid for any reason, the remainder of this Agreement will remain in full force and effect.

The terms of this Agreement can be changed only by a written modification to the Agreement by the agency signatories (or their designated representatives) to this Agreement or by the parties adopting a new agreement in place of this Agreement. The [insert name of the department/unit] Information System Security Officer will be included in coordinating adoption of new terms.

Signatures and Concurrence

On behalf of both parties, the undersigned individuals hereby attest that they are authorized to enter into this Agreement and agree to all the terms specified herein.	
Signature	Date
Printed name	
Title	Director/head]
Signature	Date
Printed name	
Title	[Participating Entity]
Signature	Date
Printed name	
Title	[Data Steward or Designee]
Signature	Date
Printed name	
Title	[Data System Owner/Designee]

Appendix A – Key Points of Contacts

Role	Name	Title	Affiliation	Contact Information (Phone with Country Code and Email)
Data Steward (or designee)				
Data System Owner (or designee)				

[Participating Entity] in Uganda				
[Department / Unit] Programmatic Point of Contact				

Appendix 2: Health Data Access, Sharing, and Use Compliance Checklist

1. Legal and Regulatory Compliance

- **Data Protection and Privacy Act 2019 Compliance:** Ensure all data access and sharing practices comply with the Data Protection and Privacy Act 2019.
 - Privacy Rule
 - Security Rule
 - Breach Notification Rule
- **Country-Specific Guidelines:** Verify adherence to any relevant country-specific health data regulations.

2. Data Governance

- **Data Ownership:** Clearly define data ownership and stewardship responsibilities.
- **Data Classification:** Classify data according to sensitivity and confidentiality.
- **Data Access Policies:** Develop and implement data access policies.
- **Data Use Policies:** Develop and implement data use policies.

3. Data Security

- **Access Controls:** Implement robust access control mechanisms.
 - Role-based access
 - Multi-factor authentication
- **Encryption:** Encrypt data in transit and at rest.
- **Security Audits:** Conduct regular security audits and assessments.
- **Incident Response Plan:** Develop and maintain an incident response plan.

4. Data Sharing

- **Consent Management:** Ensure proper consent is obtained and documented for data sharing.
- **Data Sharing Agreements:** Establish and enforce data sharing agreements with third parties.
- **Data Minimization:** Share only the minimum necessary data.
- **Third-Party Compliance:** Ensure third parties comply with all relevant regulations and standards.

5. Data Use

- **Purpose Limitation:** Use data only for the specified purposes for which consent was obtained.
- **Anonymization/De-identification:** Anonymize or de-identify data when possible to minimize risk.
- **Data Quality and Integrity:** Ensure data quality and integrity are maintained.
- **Monitoring and Auditing:** Continuously monitor and audit data use practices.

6. Patient Rights

- **Right to Access:** Facilitate patients' right to access their own health data.
- **Right to Correction:** Allow patients to request corrections to their data.
- **Right to Deletion:** Ensure compliance with requests for data deletion where applicable.
- **Right to Information:** Provide clear information about data use, sharing, and protection practices.

7. Training and Awareness

- **Employee Training:** Conduct regular training on data protection and privacy policies.
- **Awareness Programs:** Implement programs to raise awareness about data privacy and security.

8. Documentation and Record Keeping

- **Policy Documentation:** Maintain up-to-date documentation of all relevant policies and procedures.
- **Access Logs:** Keep detailed logs of data access and sharing activities.
- **Compliance Records:** Retain records of compliance with regulatory requirements.

9. Risk Management

- **Risk Assessments:** Conduct regular risk assessments to identify and mitigate potential risks.
- **Mitigation Plans:** Develop and implement risk mitigation plans.
- **Continuous Improvement:** Continuously improve data protection measures based on risk assessments and audit findings.

10. Technology and Infrastructure

- **Secure Systems:** Use secure systems and technologies for data storage and processing.
- **Backup and Recovery:** Implement robust data backup and recovery solutions.
- **Regular Updates:** Ensure systems and software are regularly updated and patched.

11. Communication and Transparency

- **Transparency:** Be transparent about data access, sharing, and use practices.
- **Stakeholder Engagement:** Engage with stakeholders (e.g., patients, healthcare providers) to ensure understanding and trust.

12. Compliance Reporting

- **Internal Reporting:** Develop internal reporting mechanisms for compliance issues.
- **External Reporting:** Ensure timely reporting to regulatory bodies as required.

