PEACE, PROSPERITY AND REGIONAL INTEGRATION

INTERGOVERNMENTAL AUTHORITY ON DEVELOPMENT

IGAD Regional Health Data Sharing and Protection Policy FRAMEWORK

OCTOBER 2021


USAID
FROM THE AMERICAN PEOPLE


IGAD


BROADREACH
health development


GLOBAL HEALTH
Innovation Center


jembi
health systems NPC


ECOWAS

FOREWORD

H.E. Workeneh Gebeyehu, PhD, Executive secretary of IGAD

The Intergovernmental Authority on Development (IGAD) was established in 1986 to respond to drought, desertification, famine and related disasters by coordinating regional cooperation among Member States and partners. Its revitalization in 1996 reinforced these interventions and expanded IGAD's mandate to provide leadership in a wide-range of development sectors focusing on peace and security; agriculture, food security, climate change and environmental protection; economic cooperation and regional integration; as well as health and social development. The region is home to over 260 million people, of which more than 50 percent are Mobile Cross Border Communities.

The ongoing COVID-19 pandemic and the previous Ebola virus epidemic in West Africa are clear examples of how infectious diseases can rapidly spread across borders and of the contributing role of cross-border human migration and travel. These experiences also highlight the importance of routine health data sharing and surveillance within and across borders to improve epidemic and pandemic control and enhance public health prevention planning in order to have an integrated region.

I am Confident that the Framework will guide the development of national policies and strategies in member states where these do not exist or strengthen implementation of existing instruments in others. IGAD will continue to Strengthen Disease surveillance, Coordinate emergency response in the region and create medium for all stakeholders and Member states in the Health Sector.

FOREWORD

Ms. Fathia Alwan,Director, Social Development Division, IGAD

The Division of Health and Social Development of IGAD has seen rapid expansion over the last decade. The Division runs several social development programs including: health, nutrition, population and development; youth, labor, employment, livelihoods and self-reliance, migration, free movement of persons; education, research and knowledge management as well as issues related to the needs of refugees, returnees, IDPs and cross-border mobile populations.

This Cross Border Data Sharing Policy Framework is very important as it is the first of its kind in Africa and allows our region to respond to Pandemics and Epidemics in a coordinated manner and prepare for outbreaks as a region, This is the collective aspirations of our Member States. Therefore, the Division will use all available means to coordinate and facilitate the implementation of this important Framework.

The division will coordinate closely with the respective ministries of Health from the Member states, development partners and relevant stakeholders to ensure implementation of this framework policy in all our member states. IGAD will build capacity for its member states at all levels to ensure a robust health system for the region.

FOREWORD

Dr. Bashir Ahmed, Coordinator, Digital Health and Health Policy

In 2018, a data sharing policy landscape review conducted in the Intergovernmental Authority on Development (IGAD) region in East Africa showed that the absence of explicit data protection laws and harmonized frameworks, Which, currently hinders accurate, consistent, easy, and efficient data sharing both within and across borders. This gap leads to numerous challenges and barriers to effective monitoring of routine health indicators for cross-border mobile populations (CBMPs), accurate and timely early detection of disease outbreaks across the region, informed planning, resource allocation, and evidence-based decision-making and consistent adherence to privacy standards.

Based on this evidence, the IGAD-RAD Expert Technical Working Group and Steering Committee recommended the development of a regional health policy to address this critical gap.

Responding to the recommendation of the Expert Technical Working Group and Steering Committee, IGAD went ahead and developed the IGAD Regional Health Data Sharing and Protection Policy Framework. The policy framework, a first of its kind in sub-Saharan Africa, lays out regulations, best practices, and processes for the safe, secure, accurate, and timely sharing of health data between different countries in the IGAD region. IGAD also developed an implementation guide to help Member States develop an actionable road map towards the implementation of the policy

The IGAD Secretariat recognizes the valuable support from its partners, we thankfully acknowledge and appreciate the funding and support received from United States Agency for International Development (USAID) and the technical support received from the Regional Data for Action initiative (RAD), The support from the GIZ/BMZ to get this document disseminated and ready for the region.

ACKNOWLEDGMENTS

The IGAD Secretariat recognizes the valuable support it has received from all those who have contributed to the formulation process of this policy framework. In particular, we thankfully acknowledge and appreciate the funding and support received from United States Agency for International Development (USAID) and the technical support received from the Regional Action through Data (RAD) partners.

Furthermore, we are very grateful to the experts from the IGAD Member States, the IGAD Secretariat, and the IGAD Specialized Institutions for their technical and strategic input towards the development of the policy framework.

IGAD would also like to extend many thanks to the Duke Global Health Innovation Center RAD Team who worked tirelessly to coordinate activities and provide consultative technical expertise throughout the policy development process.

Also, we are grateful to all the individuals from the IGAD Member States and IGAD Development Partners who provided written and/or oral feedback to the policy. IGAD also appreciates the commitment of the experts who attended the consultative workshops held in the various IGAD Member States during the formulation and finalization of the policy framework. Their valuable feedback and participation in the consultative workshops enabled IGAD to gain a wider representation of views on data sharing and important insights on stakeholder expectations from different sectors, which are reflected in the policy framework document.

We would like to appreciate the effort by the IGAD Executive Secretary Dr.Workeneh Gebeyehu, Ph.D. for his continued support and belief in digitalization and its role in regional integration.

DISCLAIMER:
This publication was produced under cooperative agreement number: AID-OAA-A-16-00073. The views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

ACRONYMS

AU	African Union
CBMP(S)	Cross-border mobile population(s)
ECOWAS	Economic Community of West African States
EU	European Union
GDPR	General Data Protection Regulation
GLOPID-R	Global Research Collaboration for Infectious Disease Preparedness
ID	Identification (such as in "ID number")
IDPS	Internally displaced persons
IGAD	Intergovernmental Authority on Development
MOH	Ministry of Health
NFC	Near-field communication
NGO	Non-governmental organization
PII	Personally identifiable information
RAD	Regional Action through Data
REC(S)	Regional Economic Community(ies)
SADC	Southern African Development Community
UN	United Nations
USAID	United States Agency for International Development

DEFINITIONS

C

CONFIDENTIALITY: Disclosure or nondisclosure of personal information "based on the principle that personal information should not be released without the consent of the person involved except as necessary" to protect that person or society.[1,2]

CONSENT: Prior stated compliance, approval, or any manifestation of a data subject who has freely, unambiguously, and expressly given a statement or clear indication, oral or written, of their wishes regarding the collection, processing, use, sharing, and/or storage of their health-related data.[3] Consent is considered informed when a data subject is provided with information in an accessible format and at a level appropriate for their education and understanding about the risks, benefits, planned uses, and potential uses of their health-related data.

CROSS-BORDER: Description of an activity, process, individual, population, institution, or other concept that involves entities from different countries or that passes, occurs, or is performed beyond the jurisdiction of one origin country and across a border between two countries.[4]

CROSS-BORDER HEALTH CARE: "Health care provided or prescribed in a member state other than that of affiliation."[5] This may require "sharing information about incidence, medical background, and history of a patient by a health-care professional in different countries."[6]

CROSS-BORDER HEALTH DATA SHARING: Data sharing (see definition 15) in which data considered as health data or health-related data (see definition 20) is shared beyond the jurisdiction of the origin country of the data. Cross-border health data sharing is not limited to instances of health data sharing across a border between two countries; it also refers to the transfer or exchange of health data between two or more countries that may or may not share geographical borders.

CROSS-BORDER MOBILE POPULATIONS (CBMPs): Groups of people who regularly, routinely, or with some frequency move between two or more countries. This includes, but is not limited to, truck drivers, migrants, sex workers, traders, victims of human trafficking, asylum seekers, and pastoralists.[7]

CROSS-BORDER PROCESSING: "Processing of personal data which takes place in the context of the activities of establishments in more than one member state of a controller or processor...where the controller or processor is established in more than one member state."[8]

D

DATA CONTROLLER: Any "public or private individual or legal entity, body, or association who, alone or jointly with others, decides to collect and process personal data and determines the purposes for which such data [is] processed."[9]

DATA MISUSE: Improper use of data, including use for undefined purposes.[10,11]

DATA PROCESSING: "Any operation performed on personal data," including data collection, recording, storing, accessing, and sharing.[12]

DATA PROCESSOR: Public or private individual or legal entity that is responsible for processing personal data on behalf of the controller in accordance with the measures implemented by the controller.[13,14]

DATA PROTECTION: "The systematic application of a set of institutional, technical, and physical safeguards that preserve the right to privacy with respect to the collection, storage, use, and disclosure of personal data."[15]

DATA PROTECTION AUTHORITY: An independent, public, supervisory authority established on a national level by each member state to supervise the application and implementation of data sharing and protection guidelines.[16]

DATA QUALITY: The characteristics or attributes of data that determine its ability to fulfill its intended use completely. These attributes may differ depending on the purpose of the data. Examples of attributes of high-quality data include accuracy, timeliness, completeness, objectivity, interpretability, and accessibility.

DATA SHARING: "Granting certain individuals or organizations access to data that contain[s] personally identifiable information" or the exchange or transfer of information, including health and other sensitive data, between at least two individuals or entities. This could include the movement of sensitive data from device to server, from device to cloud storage, or between health facilities "with the understanding that the data shared cannot be re-released further unless a special data sharing agreement" is established and agreed upon by all sending and receiving parties.[17]

DATA STORAGE: The systems used to retain data after it is collected.

DATA SUBJECT: Individual from whom data is collected directly or indirectly. These individuals can be "directly or indirectly identified by reference" of information, such as name and social, physical, or cultural characteristics.[18]

DISCLOSURE: "Occurs when identifiable information concerning an individual" or information extracted from personal data is made known to a third party. Does not include a disclosure made forcefully, inadvertently, or under unauthorized circumstances.[19]

HEALTH DATA (also referred to as health-related data): Personal data (i.e., information relating to an identified or identifiable individual) related to the overall state of health, both physical and mental, of a data subject. Health data includes "records regarding the past, present, or future state of health, data collected in the course of registration for or provision of health services, or data which associates the data subject to the provision of specific health services."[20] Health data also includes any personally identifiable information (PII) that may be collected along with data that is directly related to health.[21] Furthermore, health data includes data related to health that has been collected on an aggregate level, such as health administrative data, research data, and population health metrics, and data related to health that is collected for research purposes.

HEALTH DATA USE: The ways that "health data may be used to achieve public health goals/purposes," including collection, analysis, interpretation, and review of data to monitor epidemiological trends, inform policy and programs, and provide health services.[22,23]

DEFINITIONS

INTERCOUNTRY HEALTH INFORMATION EXCHANGE: Sharing patient and aggregate-level health data across member states. This includes "sharing information about incidence, medical background, and history of a patient by a health-care professional in different countries,"[24] patient and provider information sharing, and sharing of aggregate epidemiological and health resource data.

INTEROPERABILITY: "The ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged."[25]

MEMBER STATE: A nation belonging to a political, economic, or trade organization.[26] The current IGAD member states are Djibouti, Eritrea, Ethiopia, Kenya, Somalia, South Sudan, and Uganda.

NATURAL PERSON(S): A living, individual human being; in contrast to an artificial person, which refers to an entity given some legal rights, such as a corporation, NGO, or government organization.[27,28]

PATIENT PRIVACY: The ensuring of the security and confidentiality of medical records.[29]

PERSONAL DATA BREACH: "Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed."[30]

PERSONALLY IDENTIFIABLE INFORMATION (PII): "Data relating to an individual who can be identified directly or indirectly by the data or by linking the data to other information reasonably available."[31]

PSEUDONYMIZATION: A method of de-identification of data whereby personally identifiable information is removed from its associated data and replaced with alternate identifiers that bear no resemblance to the original personal identifiers (pseudonyms). The personally identifiable information is separated from data such that the data cannot be linked to identities (re-identified) without additional information about the process of de-identification, such as a key linking identities to pseudonyms.[32]

RIGHTS OF DATA SUBJECTS: Entitlements belonging to all data subjects that are related to the collection, use, processing, storage, sharing, or any other activity involving their personal data; for instance, rights in regard to transparency of the purpose for and means of data collection, access to information, transfer of information, and rectification or erasure of information.[33,34] These are some examples of rights, but this is not an exhaustive list of the rights of data subjects.

SECURITY: The infrastructure, technological or otherwise, that protects sensitive data.[35]

SENSITIVE DATA: All data from an individual that relates to "racial or ethnic origin, political opinions, religious or philosophical beliefs, filiations, trade-union memberships, gender, and the processing of data concerning health or sex life as well as any personal data which [is] considered by a member state as presenting a major risk to the rights and interests of the data subject."[36,37]

INTRODUCTION

PHOTO CREDIT: EMMANUEL CHANDIGA

VISION

Be the premier regional economic community for achieving peace and sustainable development in the region.

IGAD's vision is to be "the premier regional economic community for achieving peace and sustainable development in the region."[38] In line with this vision, economic cooperation, integration, and social development form the second pillar of the current IGAD regional strategy. The health and social development program, which is one of the three programs under this pillar, has an overall objective of strengthening regional mechanisms and systems for improving health and social development, thus enhancing the quality of life of people of the region toward longer life expectancy and prosperity.[39]

Within the health sector, IGAD is **mainly focused on the needs of cross-border mobile populations** (CBMPs), including migrants, internally displaced persons (IDPs), victims of human trafficking, and refugees. The CBMPs have unique challenges in terms of accessing health-care services when outside their country of origin. National health systems face challenges in monitoring health indicators for these segments of the population to meet their specific health needs. Furthermore, other than during instances of emergencies and disease outbreaks, sharing of health data beyond national borders is still not the norm. Insufficient data compromises CBMPs' access to continued care and the ability of policy makers and health-care providers to track health trends and allocate resources effectively.

IGAD is mainly focused on the needs of cross-border mobile populations (CBMPs), including migrants, internally displaced persons (IDPs), victims of human trafficking, and refugees.

IGAD, drawing from its mandate that entails harmonization and coordination of policies and programs among IGAD member states and with other regional economic communities (RECs) and receiving support from the Regional Action through Data (RAD) initiative, undertook a **landscape assessment to understand the policies, practices, and challenges regarding health data sharing in its member states**. A significant finding from this assessment was a lack of clarity in policies around health data sharing. Additionally, there were often no explicit policies on health data protection. **This lack of harmonized policies on health data sharing and protection contributes to lack of continuity of care for CBMPs and restricts effective public health planning and resource allocation**. Interviews with key stakeholders in member states did note that there were mechanisms that had been institutionalized among certain member states to facilitate sharing of information at cross-border regions. Some examples of these forums for data sharing include biannual meetings of cross-border committees where the health sector is represented.

Representatives from the IGAD member states responded to the above findings by mandating IGAD to develop a regional health data sharing policy.[40] The IGAD Regional Health Data Sharing and Protection Policy framework seeks to provide clear guidance for the member states on health data sharing via a set of universal principles that ensure that health data is adequately protected. **This framework emphasizes the rights of patients by outlining the rights of data subjects and details the roles and responsibilities of various actors and stakeholders**. Ultimately, it aims to facilitate proper data sharing practices that encourage ethical cross-border health data sharing following the highest possible standards.

The IGAD Regional Health Data Sharing and Protection Policy framework seeks to provide clear guidance for the member states on health data sharing via a set of universal principles that ensure that health data is adequately protected

The policy framework has been developed with an awareness of the dynamic, ongoing conversations in the member states around data sharing and protection. It has been informed by a series of in-person and written consultations from experts and stakeholders in member states and draws on best practices from the existing data protection laws in member states (e.g., Kenya and Uganda), the African continent such as the African Union (AU) Convention on Cyber Security and Personal Data Protection, the Economic Community of West African States (ECOWAS) Supplementary Act A/SA.1/01/10, and the Southern African Development Community (SADC) Model Law on Data Protection. It also draws from recent initiatives beyond the African continent including principles expressed in the European Union (EU) General Data Protection Regulation (GDPR) and the proposed Australian government's data sharing and release legislation, as well as best practices from intergovernmental organizations such as the United Nations (UN) and the World Bank. Guidance for best practices was further informed by international nongovernmental bodies such as Chatham House, MEASURE Evaluation, the Global Research Collaboration for Infectious Disease Preparedness (GloPID-R), and Omidyar Network.

This document is a foundational framework that IGAD and its member states will use in building out connected health systems that respond to the unique needs of citizens, especially cross-border migrant populations. It is intended to **facilitate both formal and informal data sharing and to be used to help create the right environment for data sharing to promote good practice in addressing technical, political, ethical, economic, and legal concerns that may arise**. It is to be complemented by operational guidelines that will steer its implementation, governance, and accountability. In this way, the health sector will continue to contribute to IGAD's mission of enhancing regional integration and cooperation while supporting member states' efforts to achieve peace, security, and prosperity.

PHOTO CREDIT: HOLLY POWERS/ USAID SOUTHERN AFRICA

SECTION 1: PURPOSE

A central part of IGAD's core mandate involves addressing the health concerns of cross-border migrants, internally displaced persons (IDPs), and refugees to foster integration and cooperation among member states. For this to be realized, **health-related data needs to be shared within and across borders**. Secure cross-border health data sharing in open, interoperable, and accessible formats allows use and reuse of new and existing data sets to **deliver benefits to cross-border migrant populations and member states**.

BENEFITS OF SECURE CROSS-BORDER DATA SHARING:

- promoting continuity of care for mobile and immigrant populations
- improving epidemic control
- enhancing public health planning and service provision at the member state borders

However, a data sharing policy landscape review in the IGAD region showed that **the absence of explicit data protection laws and harmonized frameworks currently limits easy and efficient health data sharing, both within and across borders**. For example, there are some concerns about sharing aggregate country-level health-related data, thus exposing it to external scrutiny, or sharing patient-level data, due to its personal and sensitive nature. This may lead to decisions not to share data or to apply unnecessary protections to the data, significantly reducing its usefulness. While these are important concerns, with appropriate risk management, they can be weighed against the potential benefits of data sharing.

Considering this background, it was found advisable to develop a regional data sharing and protection policy framework that is in line with internationally established best practices and that sets out the terms and conditions of health data transfer across member states.

This regional data sharing and protection policy framework, designed for implementation within the IGAD region, is based on similar global and regional data protection regulations such as the European Union's General Data Protection Regulation (GDPR), Kenya's Data Protection Act of 2019, and Uganda's Data Protection and Privacy Act of 2019. The policy framework is developed with the aim of establishing a clear structure for health data sharing and protection, thereby assisting IGAD member states in considering the appropriate safeguards to apply while sharing health data, maximizing the benefits of data sharing, and safeguarding the privacy and interests of individuals and the member states.

The principles described in the policy framework enable an approach to health data sharing that balances the benefits of sharing health-related data with a range of mitigation strategies that address attendant risks and promote data protection. **Applying the principles through consistent implementation of the framework** across IGAD member states, supported and facilitated by IGAD, **will enable safe and effective sharing of health data** in a way that protects privacy and maintains confidentiality while delivering maximum benefit to the patients and member states. Upon implementation in the member states, this policy framework will guide health data sharing laws, regulations, and protocols in each member state and establish commonalities between member states such that cross-border data sharing with ease, efficiency, benefit to member states' common interests, and minimum risk and harm to data subjects is facilitated.

The principles described in the policy framework enable an approach to health data sharing that balances the benefits of sharing health-related data with a range of mitigation strategies that address attendant risks and promote data protection.

POLICY STATEMENT

The IGAD Regional Health Data Sharing and Protection Policy is a policy framework that **provides guidance, recommendations, and best practices to facilitate effective and efficient sharing of health data** within the IGAD region; the framework is applicable to all instances of sharing health data, including the sharing of data both within and between countries. The policy framework outlines foundational principles of data sharing, rights of data subjects, roles and responsibilities necessary to carry out health data sharing in line with those principles and rights, and an institutional framework for governance of the policy framework and its implementation.

The purpose of this policy framework is to:

- **Facilitate an environment that enhances the secure sharing of health data** between IGAD member states at various levels—national, subnational (as defined and implemented in each member state), and individual (such as independent organizations, international NGOs, private sector entities, and natural persons)—to promote continuity of care and enable the provision of quality care across member states, improve epidemic preparedness and control, and enhance public health planning.
- **Provide guidance** on health data sharing, processing, storage, and use within the IGAD region.
- **Establish clear modalities** for health data sharing and protection across IGAD member states, including platforms and guidelines that facilitate member states' collaborative decisions on the implementation of this policy.
- **Support harmonization of data-sharing policies and practices** across the region by encouraging member states to include a section on cross-border health data sharing in their national health policies.
- **Complement laws and regulations** on privacy and personal data protection and ensure patient confidentiality when data is shared across member states.
- **Promote a multisectoral approach** to health data sharing, processing, storage, and use.
- **Serve as a dynamic instrument that can respond to future developments** in the science, technology, and practices of cross-border sharing of health-related data.

Upon uptake of this policy framework, member states shall:

- **Enact a health data-sharing policy or update existing policies** to align with this policy framework and harmonize with the policies of IGAD and other member states.
- **Refer to this policy framework for guidance** regarding cross-border health data sharing and use it as a resource when developing national processes and procedures.
- **Engage with IGAD and other member states to coordinate** regional data sharing and support continued implementation and improvement.
- Engage with IGAD and other member states to **contribute to monitoring and evaluation of policy implementation**.
- **Commit to health data sharing and protection as a strategic priority**.
- **Participate in data sharing governance structures** as needed to implement the policy framework, including appointing representatives to requisite roles for coordination with IGAD.

SECTION 2: METHODOLOGY

The RAD team conducted desk reviews and key informant stakeholder interviews and used a co-design process through expert stakeholder reviews and member state consultations to develop the policy.

Initially, the team conducted key informant interviews with international and national stakeholders across the IGAD region. Concurrently, the team did preliminary cross-border site visits with stakeholders at the subnational level in Uganda and Kenya to understand the current data sharing landscape, including operational challenges and benefits to sharing data. The team also completed a desk review of existing policies in the IGAD region related to cross-border data sharing, immunization, digital health, and migration.

Through this research, the team found **three major policy gaps** preventing effective cross-border health data sharing:

- Many countries in the region currently lack a legal or regulatory framework for cross-border data sharing.[41,42]
- The lack of a harmonized regional legal framework on data protection and storage that ensures that data is used only for the purposes for which it was intended makes the free flow of personal health data information across borders unsafe.
- The lack of consistent patient confidentiality and privacy laws across countries in the IGAD region impedes the cross-border flow of information.[43]

Using grid analysis, IGAD collaborated with partners at Duke University to select strategic approaches that improve data sharing across borders. Through the analysis, the strategic options to address the identified challenges were scored against the chosen criteria for analysis and the selected strategic approaches classified into three main clusters: policy, technical guidelines, and legal framework. The policy option was selected because it is part of IGAD's mandate and would be achieved within a shorter time frame. Furthermore, lessons from ongoing initiatives around legal agreements indicated that they would require intensive monetary and time resources to achieve consensus.

Based on the selection of the policy option, the team researched global, regional, and member state policies to identify existing regulations and best practices. Notable policies include the EU GDPR, the AU Convention on Cyber Security and Personal Data Protection, the ECOWAS Supplementary Act, the SADC Model Law on Data Protection, the Kenyan Data Protection Act, and the Ugandan Data Protection and Privacy Act.

IGAD Policy TWG/Steering Committee on Cross-border Data Policy workshop.

To further develop the policy, the IGAD and RAD teams worked with expert stakeholders and IGAD member states in a co-design process. **Experts in health, data sharing, and IT in the region commented on each draft of the policy framework to provide technical input**. The team held consultations with representatives from each member state for input and recommendations for the policy. The co-design process aimed to optimize the amount of feedback from member states to increase harmonized implementation across member states, but **the policy framework structure essentially acknowledges that member states possess unique legal and policy contexts to which this framework must be adapted upon implementation**.

SECTION 3: SCOPE

The policy framework provides guidance for activities that are related to health data sharing and protection across borders in IGAD member states. Health data is personal data (i.e., information relating to an identified or identifiable individual) related to the overall state of health of a data subject, including "records regarding the past, present, or future state of health, data collected in the course of registration for or provision of health services, or data which associates the data subject to the provision of specific health services."[44] Health data also includes any personally identifiable information (PII) that may be collected along with data that is directly related to health.[45] Furthermore, health data includes data related to health that has been collected on an aggregate level, such as health administrative data, research data, and population health metrics, and data related to health that is collected for research purposes. **Cross-border health data sharing refers to the transfer, storage, download, or other means of access of health data, at any level of aggregation, that occurs between parties within two or more member states**. This policy framework pertains specifically to health data and should be implemented in a manner that is complementary to general data governance and protection policies that may exist at the local, subnational, national, or regional level.

This document outlines best practices for health data sharing and protection, and regional harmonization thereof, toward which member states can work and provides a framework for consistent implementation of practices and policies in member states.

This document outlines best practices for health data sharing and protection, and regional harmonization thereof, toward which member states can work and provides a framework for consistent implementation of practices and policies in member states; it is not a legally binding framework. The policy framework is applicable to the sharing of health-related data that may occur in any sector; the scope is not solely limited to application within the health sectors of member states.

The guidance included in this policy framework was developed through the identification of best practices and may intersect with existing national policies in the IGAD region (e.g., Kenya and Uganda data protection laws),[46,47] other regional policies (e.g., ECOWAS Supplementary Act A/SA.1/01/10 and the SADC Model Law on Data Protection),[48,49] the African Union (AU) Convention on Cyber Security and Personal Data Protection,[50] and the European Union (EU) General Data Protection Regulation (GDPR).[51]

This policy document is suitable for adoption by member states and is written so as to be broadly applicable to different member states to facilitate ease of adoption; member states are encouraged to modify and adapt the policy framework to suit country-specific needs and contexts. **Prior to adopting and implementing the policy, member states should consider the types of health data sharing and protection activities that will be occurring between countries, the actors that will be participating in those activities, and the levels of data protection that have been implemented in other member states**. This framework provides guidelines on regional health data sharing, use, and protection best practices. However, in recognition of the different contexts across IGAD member states, countries are encouraged to adopt and further refine the policy framework to fit their specific needs, structures, and capacities, including harmonization and integration with existing data governance and protection structures and policies.

TERRITORIAL SCOPE

1. This policy framework is applicable to all IGAD member states.
2. Member states are encouraged to share health data if each country and its applicable entities have adequate and equivalent data safeguards and security measures, which are spelled out in this document.

SCOPE OF APPLICATION

1. The principles in this policy should govern the manual and automatic collection, processing, use, storage, and sharing of health data between IGAD member states and between a member state or member states and other countries that are not member states of IGAD.
2. The framework applies to the sharing of health data regardless of the sector of origin; that is, the provisions contained in this policy framework are not limited in scope to bodies and actors within the health sector, but rather are broadly applicable to any sector in which health data may be collected, processed, used, stored, or shared.
3. Individual privacy and confidentiality measures must be maintained throughout the collection, processing, use, storage, and sharing of health data across member state borders.
4. The policy framework applies to natural persons (including but not limited to citizens or stateless persons residing in member states) and public and private legal entities that will be carrying out health data collection, processing, use, storage, and sharing activities. This includes but is not limited to health professionals; facilities (e.g., clinics and hospitals); county, state, and national-level government entities (e.g., ministries of health); and international and local nongovernmental organizations.

EXCEPTIONS

1. This policy framework focuses on cross-border health data sharing. Thus, this framework does not aim to address in-country health data sharing; that is, the sharing of health data between two or more parties within one member state. However, member states are encouraged to adapt this regional policy framework and, where possible, to incorporate it into relevant national policies that apply to in-country health data sharing to promote harmonization of policies in the IGAD region.
2. This regional policy framework does not apply to the processing or sharing of health data by an individual in the context of his or her personal or household activities relating to his or her health data.

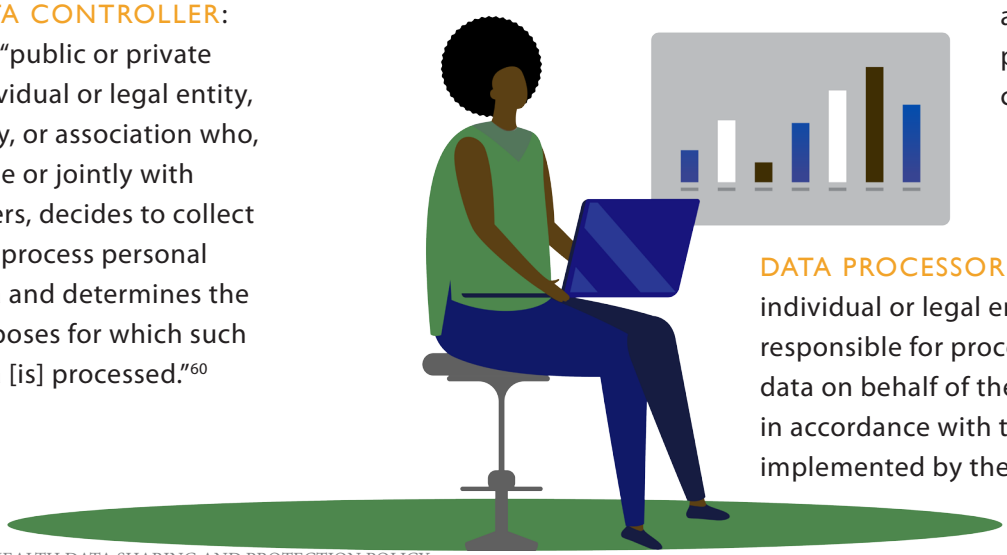
SECTION 4: PRINCIPLES OF DATA SHARING AND PROTECTION

The IGAD Regional Health Data Sharing and Protection Policy framework provides overall guiding principles underlying data sharing protection in the region. The guiding principles are informed by global (e.g., European Union, International Organization for Migration, Australia)[52,53,54] and regional (e.g., African Union, Economic Community of West African States, Southern African Development Community, African Charter on Statistics) data protection and data sharing principles and best practices,[55,56,57,58] and a series of in-person and written expert and stakeholder consultations in member states. This section outlines the guiding principles, with each principle followed by a description of related best practices.

KEY TERMS

DATA SUBJECT: Individuals from whom data is collected directly or indirectly. These individuals can be "directly or indirectly identified by reference" of information, such as name and social, physical, or cultural characteristics.[59]

DATA CONTROLLER: Any "public or private individual or legal entity, body, or association who, alone or jointly with others, decides to collect and process personal data and determines the purposes for which such data [is] processed."[60]



DATA PROCESSOR: Public or private individual or legal entity that is responsible for processing personal data on behalf of the controller in accordance with the measures implemented by the controller.[61,62]

OVERVIEW OF PRINCIPLES

1 PRINCIPLE OF PURPOSE AND RELEVANCE

Data must only be collected, processed, and shared for specific, defined, and legitimate purposes that are communicated clearly to data subjects prior to data collection, processing, or sharing. Only data that is necessary and relevant for the defined purposes should be collected, in the smallest amount necessary to achieve those purposes.

2 PRINCIPLE OF DATA QUALITY

A common minimum quality standard for data should be established, including dimensions of accuracy, completeness, consistency, validity, uniqueness, and timeliness.

3 PRINCIPLE OF LEGITIMACY, TRANSPARENCY, AND CONSENT

Processing of data must be carried out through legitimate means and in a transparent manner. Informed consent from data subjects must be obtained and recorded for their personal data to be collected, processed, or shared.

4 PRINCIPLE OF ACCESS

Access permissions must be clearly defined by data controllers and processors, including guidelines for how authorized individuals may access personal data, the nature and scope of activities that are permitted under each authorization, and the process by which an individual may receive authorization to access personal data.

5 PRINCIPLE OF CONFIDENTIALITY, STORAGE, AND SECURITY

Data must be protected from loss, damage, destruction, and unauthorized access and use through organizational and technical data security measures. Data should not be kept for longer than is necessary for its intended purpose and should undergo de-identification measures for confidentiality.

6 PRINCIPLE OF DATA SHARING AND TRANSFER

The purpose and the specific parties involved in sending or receiving data must be clearly defined when pursuing a data transfer. Data should be transferred using protected means of communication and in an accessible, machine-readable, standardized, timely, and interoperable format to maintain data protection across sending and receiving parties.

7 PRINCIPLE OF ACCOUNTABILITY

Organizations are responsible for adhering to the above principles, and associated data controllers should be able to demonstrate compliance with these principles.

PRINCIPLE OF PURPOSE AND RELEVANCE

Data that is to be shared across borders must only be collected, processed, and shared in a lawful manner by mandated institutions and for a specific, defined, and legitimate purpose. The purpose for which health data is needed should be made clear before data is shared. Data subjects must be informed of the purpose(s) for data collection, processing, and sharing as well as the benefits and risks so that they understand the value of sharing and how the data will be used. **Health data use and disclosure are limited to their intended purpose(s) and should not be processed in a way incompatible with this/those purpose(s) unless the data subject gives consent for further use.**[63,64] Exceptions for the requirement for consent are listed under "Principle of Legitimacy, Transparency, and Consent." Only data that is necessary and relevant should be collected. The smallest amount of data necessary to achieve the purpose should be considered. Collecting extra data because it might be useful later, or simply because no thought has been given to whether it is necessary, should be avoided.

RECOMMENDATIONS & BEST PRACTICES

Governments should develop standards for data collection and management.[65] Standards should include in what form the data can be used (e.g., aggregate) and whether or not consent is required for the use.[66] The ECOWAS Supplementary Act states that controllers and processors must provide the justification for and purpose of data collection and use, the means by which data can be collected, and the types of information prohibited from collection.[67] Article 5 of the GDPR also states that data must be processed lawfully and collected for specific purposes.[68]

Governments should develop guidelines to determine the legitimacy of purposes for health data use and sharing, including provisions to safeguard data subjects from malicious or unlawful uses of their health data. The Australian government's "Best Practice Guide to Applying Data Sharing Principles" suggests the use of a purpose test to determine if data sharing is appropriate.[69] According to the Chatham House data sharing guide, making potential benefits explicit, such as improvements in public health and opportunities for collaboration, can encourage data sharing.[70]

PRINCIPLE OF DATA QUALITY

Health data collection, processing, and sharing must be conducted with a minimum quality standard, which should be shared across stakeholders and member states. **The key dimensions of quality include accuracy, completeness, consistency, validity, uniqueness, and timeliness.**[71] Data does not have to be "perfect," but data should be of high enough quality for the intended purpose, considering accuracy of data collection and entry, completeness of data according to the established purpose and required data collection parameters, and consistency of collection methods and metrics.

To establish validity of data, the type of data collected, including the definitions of metrics that are included in data sets, should align with established standards in the field or sector and be pertinent to the data's intended purpose. Data should also be unique, such that entries are not repeated or duplicated within the data set.

Data uniqueness can be achieved through careful data collection processes and data cleaning to remove any duplicated data. Static assessment of data uniqueness can be carried out by determining if duplicate records currently exist in a data set that has already been collected and entered, during the process of data cleaning. Continuous monitoring of data uniqueness requires procedures to locate exact or potentially matching records during data collection and entry processes and thus prevent the entry of duplicate data prior to the data cleaning stage.[72] Finally, health data must be shared on an agreed-upon timeline so that the data subject or the public receives the maximum benefit from the shared data, which includes receiving quality health services. Once data sets are sufficiently informative and quality controlled, they should be released as quickly as possible. While quality is important, it needs to be balanced with timeliness. The time needed may vary depending on the situation, the complexity of the data, and the need for sufficient quality assurance. A feedback mechanism should be established to further improve data quality whereby data controllers, processors, and other stakeholders to whom data sets are accessible can provide comments and suggestions to improve data quality or flag data quality issues to the relevant parties in a systematic manner. Countries should consider providing incentives to ensure timeliness and quality of data.

RECOMMENDATIONS & BEST PRACTICES

The GloPID-R principles for data sharing in public health emergencies state that data providers must ensure a minimum quality standard of data and that data users must conduct any data processing, sharing, or analysis with quality standards that are equal to or greater than the minimum. Further, the principles state that data providers and users must adhere to appropriate and recognized data standards.[73] Technical and human resource factors influence data quality; therefore, standardization and automation should make sharing easier, more efficient, and more effective. Stakeholders should make certain that resource requirements are met to ensure data quality is sufficient to achieve the intended public health purpose.[74] The principle of timeliness refers to the ability to mobilize resources and knowledge in an efficient and rapid manner to respond to public health emergencies. Suggestions for a timely response for sharing data include use of harmonized protocols and development of outlines for how and with whom data will be shared.[75]

PRINCIPLE OF LEGITIMACY, TRANSPARENCY, AND CONSENT

Processing of health data may only be carried out on a legitimate basis and in a fair and transparent manner. **The communities and individuals from whom the data originates should be kept informed about how their data is collected, analyzed, used, stored, protected, and disposed; they should additionally be informed of data privacy measures that have been applied to their data and the ways that these measures protect and benefit them**. Whenever possible, data subjects must be notified at once about any personal data breach that is likely to adversely affect the data subjects.[76] This should be done in writing or orally and in a manner and language that are understandable to the data subject. Any alternative data uses that have not been considered or that do not form part of the initial sharing agreement should be discussed and agreed upon by all parties prior to any such use. There should also be accountability that allows redress if data misuse has occurred.

Data subjects must consent to the collection, processing, and sharing of their personal health data. Consent must be obtained and recorded in an ethical, agreed-upon manner (e.g., orally, in writing, or via electronic method), preferably at the time of collection.[77,78] Meaningful consent involves the consent giver having a substantive understanding of exactly what they have consented to, including all of the personal risks involved.

If data subjects, for any reason, are not fully capable of understanding and expressing their will, the informed consent should be replaced by other equivalent measures. The option to not provide consent for data sharing ("opting out") should be openly and clearly outlined and communicated to data subjects prior to requesting consent, as a required step in the process.

Consent should be managed in a way that balances public health benefits with individual privacy concerns. The requirement for consent may be waived if the collection and use are clearly in the interests of the individual and consent cannot be obtained on time; if disclosure is needed to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records; or if the processing is necessary for public health reasons. However, even under circumstances where consent is waived, processing of data should only be undertaken in line with the outlined safeguards and principles, including transparency. A data protection impact assessment, which considers any adverse effects on individuals, should also be undertaken.

RECOMMENDATIONS & BEST PRACTICES

Article 23 of the ECOWAS Supplementary Act dictates the principle of consent and legitimacy, stating that "Processing of personal data shall be considered legitimate where the data subject has given his consent." Article 23 also includes conditions for waiving the consent requirement.[79] Similarly, Article 5 of the GDPR provides principles for processing data, which also include requirements such as consent of the data subject.[80] The International Covenant on Civil and Political Rights requires states to respect the right to privacy but recognizes that states can waive the right to privacy for public health reasons.[81]

PRINCIPLE OF ACCESS

The sensitive nature of health data necessitates that data controllers and processors, prior to granting access to data, must clearly define the categories of persons who may have direct access to the data based on service function or responsibility; guidelines for how those individuals may access personal data; and processes for receiving authorization to access the data.[82] Access to data refers to the ability to locate, retrieve, obtain, read, modify, copy, or move data. Authorized individuals may also have access to shared data and may be permitted to share data by the data controller.[83] The data subjects must have appropriate rights to information access, correction, deletion, and objection;[84] the processes to exercise these rights should be clearly and accessibly communicated to data subjects and should be designed such that barriers are minimized and data subjects are empowered to exercise these rights without undue burden.

RECOMMENDATIONS & BEST PRACTICES

Article 7 of the ECOWAS Supplementary Act indicates that requests for authorization must specify categories of persons having direct access to recorded data and the functions of persons or departments who will have access.[85] Other best practices dictate that electronic access to sensitive data should be restricted using passwords and/or two-factor authentication.[86] The Australian government's "Best Practice Guide to Applying Data Sharing Principles" indicates that all individuals who may have access to data must undergo an authorization process that assesses the individuals' knowledge, skills, and motivations. All individuals must be trained on best practices and how to appropriately access, use, and disclose data.[87]

PRINCIPLE OF CONFIDENTIALITY, STORAGE, AND SECURITY

Health data must be subject to proper security safeguards and protected from loss, damage, destruction, and unauthorized use. Appropriate organizational (e.g., principles, policies, procedures, processes, and controls) and technical (e.g., physical devices, hardware, and software) data security measures must be put in place.[88] **Data controllers and processors must implement appropriate structures to limit disclosure of personal health data to unauthorized individuals or organizations to ensure the confidentiality and integrity of personal health data**. Sufficient security measures that are appropriate for the type, purpose, and format of health data enable rigorous implementation of the Principle of Access.

To protect data subjects from attacks on their privacy, dignity, and even safety, all decision makers— including health project designers, implementers, system designers, and developers—should consider data privacy issues upfront and integrate privacy into the design of healthcare projects and applications and throughout the life cycle of any system, service, product, or process.[89]

Health data can become a liability due to increased security risks and infrastructure costs if it is retained beyond what is "necessary." Holding onto data longer than needed also increases the risk of using the data for purposes other than that for which it was originally collected, merely because it is still available and accessible. However, disposing of data prematurely (especially historical data) can lead to the loss of valuable insight. Health data should, therefore, not be kept longer than required for the intended purpose, but for a period in line with the storage laws of the member state in which the data is stored. If there is no national guidance, then personal data should not be kept for longer than necessary for the purpose for which it was originally obtained. Any exceptions to this must be extremely limited and clearly defined, and privacy implications for the data subjects should be carefully considered.

If storing data outside of the member state in which it originated, the data protection authority of the origin country should verify the effectiveness of the security safeguards of the data storage methods in the country to which the data is transferred and in which it will be stored. Storage or processing of health data outside of the origin country should occur only upon confirmation of proper safeguards and security measures.[90] Regional-level data that includes data from more than one origin country should be stored according to standards of security that have been agreed upon by all origin countries.

Both aggregated and disaggregated data must be de-identified. Pseudonymization can be used in combination with de-identification to further enhance privacy. Data sets can be de-identified by removing from the data unique identifiers such as names, addresses, and other information that could be linked to individuals or organizations or through pseudonymization, whereby in addition to being removed, any identifying characteristics of the data are replaced with pseudonyms, thus reducing the likelihood of the linking of a data set with the original identity of an individual. Member states should not make any attempt to re-identify data. If inadvertently done, parties should be informed at once, and the information should not be used.

RECOMMENDATIONS & BEST PRACTICES

The Australian government has developed a de-identification decision-making framework as a practical guide to best practices in de-identification.[95] Other best practices include providing clarity on how and when personal data will be shared and outlining risk mitigation strategies for these situations.[96] While guidelines that call for de-identification as a best practice exist in Africa, there has not yet been established a standardized guide or framework outlining specific recommended steps to carrying out de-identification.

Upon a data breach or compromise of data security—that is, when the health data of a data subject has been accessed by an unauthorized party—the data protection authority should be notified, and a decision must be reached about how the affected data subject should be notified. Governments should consider forming or engaging a technical working group or governance committee that would be responsible for monitoring, documenting, and responding to data breaches and developing standard operating procedures that include instructions for responding to data breaches.[101] The EU GDPR instructs that data controllers must report a data breach to a supervisory authority within 72 hours, and if the breach is reported after 72 hours there must be adequate reasons for the delay. When notifying the data controller of a breach, the data processor should describe the nature of the data breach, communicate the name and details of the data protection officer, and describe the consequences of the breach. Data breaches must be reported to the data subject if they are likely to affect the rights or freedoms of the subject or other persons.[102]

Kenya's Data Protection Act specifies that data processors must alert data controllers within 48 hours of becoming aware of a data breach, that data controllers must alert the data protection authority within 72 hours of becoming aware of a data breach, and that notification that falls outside of these time periods must be accompanied by reasons for the delay. Notification of a data subject must include information on the nature of the data breach, the measures that will be taken to address the breach, recommendations for measures that the data subject could take to mitigate the effects of the breach, the identity of the unauthorized party (where applicable), and the name and contact information of the data protection officer or the appropriate individual to contact for more information.[107] Uganda's Data Protection and Privacy Act states that data subjects should be notified via registered mail, electronic mail, placement in a prominent position on the website of the responsible party, or through publication in mass media.[104]

Article 25 of the ECOWAS Supplementary Act includes a statement that data should not be kept longer than for the intended purposes of its use.[91] Some research initiatives, such as MEASURE Evaluation, recommend mitigating security risks by limiting the amount of data that is stored on a specific device and encrypting messages that contain personal data, such as test results.[92] Kenya's Data Protection Act specifies that a data controller or data processor may transfer personal data to another country only after providing the data commissioner with proof of appropriate safeguards in terms of data protection measures and the data protection laws of the country to which the data is transferred, or if the transfer is necessary to complete a contract of the data subject; for public interest; for the establishment, exercise, or defense of a legal claim; in order to protect the data subject if the data subject is physically or legally incapable of providing consent; or for "the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights, and freedoms of the data subjects."[93] Uganda's Data Protection and Privacy Act also outlines requirements that the data processor or data controller verify that the country in which data is processed or stored "has adequate measures in place for the protection of personal data" and that the data subject has consented when processing or storing data outside of Uganda.[94]

Identification systems that use unique identification (ID) numbers present opportunities for standardized pseudonymization of data by replacing identifiers such as names with data subjects' ID numbers, given that these ID numbers are secure, reveal no personal information, and are not linked to data subjects' identities in ways that are widely known or easily discovered. According to the World Bank, generating unique ID numbers using a randomized number structure is the best practice to optimize privacy and security.[97] However, unique ID numbers may pose confidentiality and security risks if used across multiple systems, since association with varied data sets increases the likelihood of an ID number being linked to a sufficient level of otherwise separate information to correlate personal information to an individual's identity. To reduce this risk, ID numbers should be used solely as identifiers and not for other purposes, such as authentication (referred to as "function creep"). There should be policy, regulatory, and legal measures in place to enforce the appropriate use of unique ID numbers and technical measures to obscure unique ID numbers when they are used.[98] Kenya's National Integrated Identity Management Scheme (NIIMS), through which each person would be assigned a unique Huduma Number that identifies them and provides access to public services, is an example of a proposed unique ID system. Jembi Health System's Journey Solution is another example of a unique ID system that stores patient immunization records as de-identified electronic personal health records (ePHR) associated with near-field communication (NFC) cards that patients can physically carry with them.[99] An appropriate regulatory framework concerning implementation of unique ID systems such as these that addresses data protection, data breaches, security, and privacy and also safeguards data subjects' rights must be in place so that the systems do not introduce additional risks to the population. Function creep and access to and retention of data should be closely monitored and controlled as part of this regulatory framework.[100]

PRINCIPLE OF DATA SHARING AND TRANSFER

Data controllers and processors must provide clarification of whether instances of health data transfer in cross-border areas require authorization, must dictate which individuals may send or receive data, and must identify the purpose for sharing data when pursuing a transfer. **The data should be transferred using only protected means of communication and confidentiality should be kept throughout transmission**. To facilitate efficient use, data should be transferred in an accessible, machine-readable, standardized, timely, and interoperable format.[105,106,107,108]

Regarding intercountry data sharing, the receiving country or organization must ensure an adequate level of data protection that considers national legislation, data protection rules and security measures, national security, and the rights of the data subject and the public.[109,110,111,112] Additionally, data controllers and processors must clearly define relevant technological concepts and relevant activities that are or will be conducted in data transfers.[113]

RECOMMENDATIONS & BEST PRACTICES

Recommendations and Best Practices: The GDPR advises that, at the regulatory level, an independent supervisory authority could exist to ensure and enforce compliance with data protection rules across organizations and borders.[114] Article 19 of the ECOWAS Supplementary Act recommends that a data protection authority, as described in Section 5 that follows, be vested with the power to authorize transborder transfers of data.[115] Article 36 of the ECOWAS Supplementary Act A/SA.1/01/10 places the responsibility for transferring data across borders with the data controller.[116] Other best practices include the creation of guidelines to assess electronic and physical security protections and methods of data transfer and storage to ensure protection of personal data. Data can be electronically transferred using end-to-end data encryption, using secure transfers such as HTTPS, or with a digital signature. Further, security keys that are used to transfer data electronically should contain at least 128 bits. [117]

PRINCIPLE OF ACCOUNTABILITY

Organizations and the data controllers of those organizations are accountable for ensuring that the above principles are followed when storing, processing, transferring, or otherwise accessing health data. Data controllers must be able to clearly demonstrate compliance with any and all of the provisions outlined in this policy framework, upon request.

RECOMMENDATIONS & BEST PRACTICES

Recommendations and Best Practices: The GDPR includes accountability as a principle, requiring that organizations implement appropriate measures to enable adherence to regulations and that they are able to demonstrate these measures and their effectiveness. The European Data Protection Supervisor, the independent data protection authority of the EU, suggests measures that organizations and data controllers can take to increase their accountability and enable them to demonstrate compliance with GDPR requirements. For example, documentation of processes and procedures around data protection, including what data are processed, when, and by whom, and integrating a role dedicated to data protection, such as a Data Protection Officer, into organizational planning could help an organization improve its level of accountability.[118]

SECTION 5: RIGHTS OF THE DATA SUBJECT

PHOTO CREDIT: THE WOT-IF? TRUST

The rights of the data subject are **entitlements belonging to the data subject regarding the processing of their personal health data**. Within this policy, it is recommended that data subjects should have the right to information, the right of access, the right to data portability and free transfer, the right to rectification and erasure of information, and the right of objection.[119,120,121]

The rights of data subjects are not limited to the five rights outlined in this section. These five rights are foundational to the cross-border sharing and protection of health-related data and are necessarily complemented by other human and civil rights outlined in or guaranteed by national policies of IGAD member states or other applicable international policies, standards, or agreements. **The five rights included in this section pertain to processes that occur once data has been collected**. Additionally, there are cases in which the rights of data subjects may be restricted in consideration of public interest or security, legal or regulatory obligations, voluntary waiver of rights, and existing public availability of data.

Protecting the rights of vulnerable populations is of particular importance. **To support enactment of these rights for vulnerable populations and to ensure that the five rights are appropriately and consistently protected for all data subjects**, additional care should be taken to account for communication barriers that may result from differences in language or culture between parties. Measures such as proactive, intentionally designed, and continuing education and training should be implemented to mitigate potential challenges, and these measures should be evaluated and revised periodically.

This section outlines the five key rights of data subjects, exceptions to those rights, and related best practices.

RIGHT TO INFORMATION

The data subject has the right to:

1. Obtain information related to their personal health data.
2. Obtain information regarding the purpose of collection, processing, storage, and use of the health data in a format and at a level of explanation that is appropriate for the data subject's understanding.
3. Obtain information regarding the potential disclosure and transfer of their personal health data.
4. Receive written notification of a personal data breach, or any data breach or compromise of security of a data set including their identifiable data, that provides sufficient information to allow the data subject to understand the extent and nature of the breach and take measures to prevent or otherwise mitigate potential consequences of the breach within a reasonably practical period after data controllers become aware of such a breach.
5. Obtain contact details of the data controller, processor officer, or other authority.[122,123]

RIGHT OF ACCESS

The data subject has the right to, upon request:

1. Access their health data and information about the data through reasonable means and timeliness and without undue payment or hardship.
2. Confirm if the data is being processed.
3. Receive communication about the manual or automatic processing of the health data and the processes taken to do so.
4. Access all information included in the Right to Information.[124,125,126]

RIGHT TO DATA PORTABILITY AND FREE TRANSFER

The data subject has the right to:

1. Obtain their personal health data from the data controller to whom the data was provided, in a structured, commonly used, and machine-readable format.
2. Transfer that data to another data controller or processor freely and without hindrance.
3. Have that data transmitted directly from one data controller to another data controller upon request, if technically feasible.[127,128]

RIGHT TO RECTIFICATION AND ERASURE OF INFORMATION

The data subject has the right to:

1. Authorize the rectification, update, or destruction by a data controller or other data authority, where technically feasible, of health data shown to be inaccurate, incomplete, questionable, unlawful, or outdated.
2. Withdraw the consent given before data collection and request that related data obtained based on that withdrawn consent be erased.
3. Limit the access to and disclosure of inaccurate, incomplete, questionable, unlawful, or outdated health data.[129,130,131]
4. Be informed about the rectification of his or her health data.[132]

RIGHT OF OBJECTION

The data subject has the right to, upon request:

1. Object to the processing of their health data for legitimate reasons.
2. Be informed prior to the disclosure of their health data for the first time and object to its disclosure or use. [133,134,135]

RECOMMENDATIONS & BEST PRACTICES

The EU GDPR also includes the right to data portability, meaning that the data subject has the right to receive their health data in a commonly used format and has the right to transfer the data to another data controller. The data subject has the right to request that this data is transmitted directly between controllers.[136] A data subject must contact a data controller or processor according to a standard, established process to exercise the right to rectification and erasure and the right of objection. Uganda's Data Protection and Privacy Act stipulates that such a notification must be made in writing.[137]

EXCEPTIONS

The rights of the data subject and obligations of the data controller or processor may be restricted by a member state's relevant national authority when data sharing and processing would safeguard the rights, freedoms, interests, or protection of the public; when an individual has given free, informed, and express consent to the restriction or waiver of his or her rights; when the data is already publicly available; and/or when it is necessary for a legal or regulatory obligation.[138,139]

Examples of situations where exceptions might be granted include:

- public security challenges
- instances when the data has already been made publicly available through legitimate, legal means, such as through processes that conform to data sharing and protection policies, standards, guidelines, protocols, and agreements in addition to relevant laws; and
- instances when individual consent for an exception has been granted.

The legitimacy of an instance of the restriction of data subject rights can be determined by applying the following three-part test: for a restriction of rights to be considered legitimate, it must be provided for by law, in pursuit of a legitimate aim, and, thirdly, necessary to secure that aim, meaning that there must be a "pressing social need" for the restriction. The reasons given to justify the restriction must be "relevant and sufficient," and the restriction must be proportionate to the aim pursued.[140]

RECOMMENDATIONS & BEST PRACTICES

Recommendations and Best Practices: Exceptions to standard data collection processes and guidelines may also occur in the cases of vulnerable populations who lack access to resources required to carry out data collection as usual; for instance, vulnerable populations may lack the means to obtain and present official identification required for consent to health data collection. Such populations retain the rights of data subjects outlined in this section. Omidyar Network's Good ID framework outlines the need for digital identity systems that both promote individual rights and ensure adequate data protection.[141] The World Bank's Identification for Development (ID4D) project has also developed principles for ID systems that will support sustainable development, which include "safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework; establishing clear institutional mandates and accountability; and enforcing legal and trust frameworks through independent oversight and adjudication of grievances."[142]

SECTION 6: ROLES AND RESPONSIBILITIES

All entities handling the processing and sharing of health data should comply with the data sharing and protection principles outlined in Section 4. In addition, many health-care professions have codes of ethics that guide practitioners in addressing common ethical questions. All health practitioners are expected to adhere to the specific code of ethics that guides their profession when processing data.

ROLES: DATA CONTROLLERS AND PROCESSORS

There are two main roles that an entity (person, organization, etc.) processing data can undertake: data controller or data processor. The key factor that defines whether an entity takes on the controller or processor role is who exercises overall control of the purposes and means of the processing of personal data; that is, who makes the final decision of what data to process and why. Data controllers are the main decision makers. They exercise overall control over the purposes and means of processing health data and shoulder the highest level of compliance responsibility. Data processors, meanwhile, handle data on behalf of a data controller and under the controller's instruction. Entities should consider whether they are acting as a controller or processor concerning their data processing activities as there are differences in the obligations and liabilities between the two.

DATA CONTROLLER

Data controllers include any **public or private individual, legal entity, body, or association**—at health provider, facility, district, state, national, regional and/or international level—who, alone or jointly with others, decides to **collect, process, or share health data**, regardless of whether such data is collected, stored, processed, or disseminated by that party or by an agent on its behalf.

Data controllers are responsible for **determining the purposes and means of processing health data and implementing technical and organizational measures** that ensure that the processing of health data takes place within the framework of data sharing and protection principles.

JOINT CONTROLLERS

If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are **joint controllers**. However, they are not joint controllers if they are processing the same data for different purposes. Joint controllers must arrange between themselves who will take primary responsibility for ensuring compliance of the data sharing and protection principles.

ACCOUNTABILITY

Data controllers remain accountable for health data under their control without regard to the location of the data and should take all appropriate measures—including when the processing is outsourced—to ensure that the data is secure. Controllers are responsible for the compliance of their processor(s) to the data sharing and protection principles.

DATA SHARING AGREEMENTS

Data sharing agreements should be made **between the controller and the organizations/individuals receiving the data sets**. The agreements should comply with the national laws of all countries involved, regional and global legislation, and any other legally binding agreements, and should properly consider the rights and interests of all parties. The agreements can take different forms depending on the nature of the data being shared, any pre-existing relationship between stakeholders, and whether the agreement needs to be binding. This could range from an informal agreement at the local, technical level to a formal ministerial authorization. Formal data sharing agreements are not necessary if informal arrangements are sufficient to accomplish the goal of sharing. However, it is important to ensure that signatories to the agreement have the necessary authority.

Data sharing agreements can help to **protect the controller and ensure the data is not misused** while helping all parties be clear about their roles.

Data sharing agreements should specify:

- what the data can and cannot be used for
- the period of agreement (i.e., when the provider will give the data to the receiver and how long the receiver will be able to use the data)
- the methods that the receiver must use to maintain data security and ensure that the data remains confidential
- any resulting public health actions
- any sanction that may be imposed if the terms and conditions of the agreement are not met.

In addition, data sharing agreements should include information about how the purpose test is satisfied.

It is best practice to make data sharing agreements publicly available to maximize transparency. After the data has been processed and shared, it is important to evaluate whether the uses and outcomes match expectations.[143]

CONSENT

The data controller must be able to **demonstrate that the data subjects have consented to the processing of their data and should provide timely responses to inquiries** (either in the form of complaints or requests for information) by a data subject. Controllers are responsible for providing notice, as appropriate, to data protection authorities or other relevant authorities when there has been a significant security breach affecting personal health data. When the breach is likely to adversely affect data subjects, a data controller should, whenever possible, immediately notify the affected data subjects.

Data controllers should carry out data protection impact assessments on a routine basis.

DATA PROCESSORS

WHO

Data processors **act on behalf of, and only on the instructions of, the relevant controller, using the measures implemented by the controller**.[144,145] Data processors may belong to the same institution or body as the data controller.

WHAT

Best practices dictate that the carrying out of data processing by a processor should be governed by a contract or other legal act as per the member state law. Processors should not share data with other third parties or engage with other processors without authorization from the controller. They should process personal data based on documented instructions from the controller while ensuring data confidentiality.[146]

The data processor, with the permission of the controller, can **delegate all or part of the data processing requested by the data controller to a data subprocessor**, who will be governed by the same conditions set out by the controller.

Data processors will normally have no independent reason to hold and process the data; they do so only to perform a service for the data controller. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under the member state law to which the processor is subject.

RESPONSIBILITIES

To ensure the successful implementation of the data sharing and protection policy, **various stakeholders will need to take part in its implementation**. What follows is a list of key actors and their expected responsibilities with regard to ensuring the implementation of the principles outlined in the policy framework.

MEMBER STATES

- Member states should **review as needed and, where appropriate, adjust their health policy frameworks** to ensure that a section on intercountry sharing of health data is included and that it is in accordance with the data sharing and protection principles to promote secure sharing of personal health data.
- Member states are encouraged to **develop and/or promote the adoption and implementation of strategies and/or legal instruments** that protect data privacy and that reflect a coordinated approach across governmental bodies.
- Member states and their institutions should **share data periodically based on priorities agreed upon within the IGAD region**. They should take all reasonable and appropriate steps to ensure that intercountry flows of health data between member countries are uninterrupted and secure. Mechanisms to promote longer-term, sustainable health data sharing should be considered alongside more immediate goals.
- Member states should provide for **adequate sanctions and remedies** in case of failures to comply with laws protecting privacy.
- Member states should **establish and maintain data protection authorities** to uphold data protection rights within the country. These authorities should have the resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial, and consistent basis. These authorities should coordinate regularly with the ministries of health through an assigned focal point for health data.
- Each member state should support its ministry of health to **establish a data sharing technical committee or similar coordinating body** that can oversee and provide guidance on cross-border sharing of health data in accordance with the principles outlined in this framework. Each member state should also support its ministry of health to appoint a focal person to engage with national data protection authorities.
- Member states should r**efrain from restricting intercountry flows of health data** between their countries and another country where sufficient safeguards exist. Effective enforcement mechanisms and proper measures should be put in place to ensure a continuing level of protection consistent with data sharing and protection principles.
- Member states should **consider the adoption of complementary measures**, including awareness and literacy regarding data sharing benefits and consequences, skills development, and the promotion of technical measures that help to protect the privacy of health data.
- Member states should **encourage and support the development of international arrangements** that promote interoperability among systems and data privacy and protection frameworks and that give practical effect to the outlined data sharing and protection guiding principles.
- Member states should **carry out dynamic monitoring and evaluation** to assess how their domestic data infrastructure systems are supporting cross-border health data sharing and data protection.
- Member states should **identify gaps** in financial, technical, and human resource capacity and **implement measures** to address them.
- Member states should **work with existing governmental bodies** with expertise in data control and process and involve ICT authority when considering how the roles outlined in this policy will be actualized in member states.
- Member states should seek to **engage private-sector apex bodie**s within each respective country to ensure that their members—private health facilities, private insurers, and private practitioners—understand the goals of this policy.

- Given the significant contribution of the private sector in health service provision, member states should **develop a stakeholder engagement strategy that includes the private sector**. The stakeholder engagement strategy should include ways to incentivize the private sector to provide health data consistently and report it to national health information systems.
- Ministries of health within member states should **define other sources of health-related data** within the country. Each member state should also identify government ministries and units that generate health-related data and develop operational guidance on how ministries of health will coordinate with other sectors to ensure that health-related data is shared, collated, analyzed, and stored in line with this policy.

COMMUNITY MEMBERS

- All citizens and patients should be **actively engaged in ensuring that their health data is protected and shared safely**.
- All citizens and patients should ensure that they are **kept updated on their rights** regarding health data sharing and protection and also ensure that resources earmarked to support data sharing and protection are used in the manner intended.

HEALTH FACILITIES AND FRONTLINE HEALTHCARE WORKERS

- Health facilities and frontline healthcare workers in member states should be engaged in the **implementation of this policy** given that significant amounts of health data are generated at this level of the health system.
- Ministries of health within member states and other institutions involved in implementing this policy should **develop operational guidance on how to interface** with frontline healthcare service providers and health-care facilities.

PRIVATE SECTOR AND NON-HEALTH SECTOR

- The private sector and non-health sector should **coordinate with ministries of health** to ensure that health-related data is shared, collated, analyzed, and stored in line with this policy.

IGAD

- IGAD shall **provide oversight** and stewardship to the implementation of the regional health data sharing and protection policy framework.
- IGAD shall **advocate for member states** to enact health data sharing and protection policies and encourage member states' continued engagement through workshops.
- IGAD shall work with member states to **encourage and support the development of international arrangements** that promote interoperability among systems and data privacy and protection frameworks and that give practical effect to the data sharing and protection guiding principles outlined in this policy.
- IGAD shall **promote cooperation** with the member states that do not yet have independent supervisory data protection authorities.
- IGAD will **support the building of data infrastructure** for member states to a minimum standard.
- IGAD shall, on an ongoing basis, **monitor and communicate relevant developments** in the member states, other countries, and international organizations insofar as these developments have an impact on secure sharing and processing of health data, and advise member states on strategies to help negate any negative impacts.

SECTION 7: INSTITUTIONAL FRAMEWORK (GOVERNANCE)

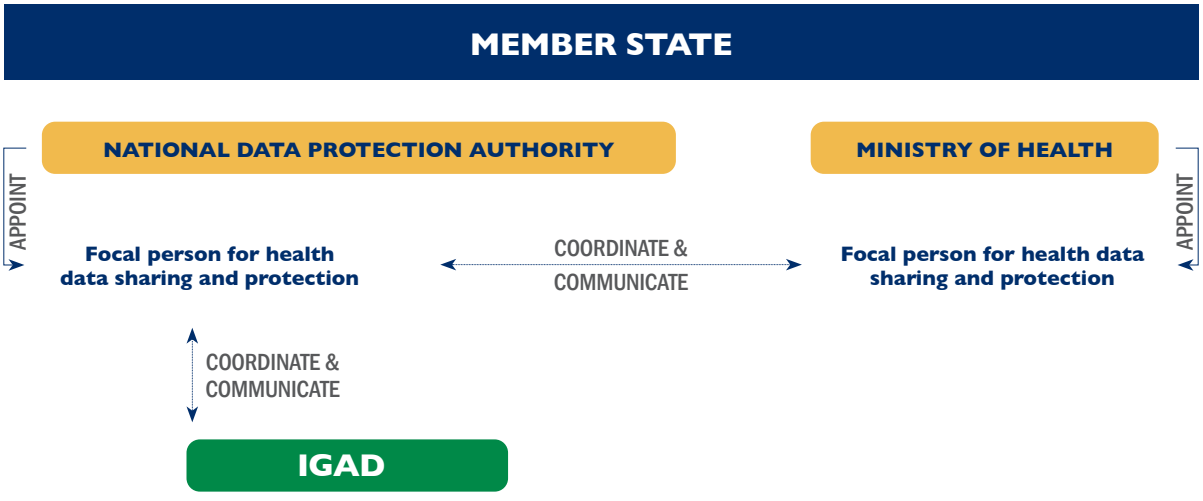
Within the IGAD region, **each member state is encouraged to establish its own national data protection authority** (if such a national body does not yet exist) and provide for adequate sanctions and remedies in case of failures to comply with laws protecting data privacy in its national territory. Such national data protection authorities should be tasked with the **implementation of data protection laws** (where these are in force).

> EXAMPLE:
> *Chapter 6 of the GDPR establishes data protection authorities as independent public authorities in each member state that supervise the application of the data protection guidelines provided for in the law.[147] In the IGAD region, Kenya's Data Protection Act similarly establishes an Office of the Data Protection Commissioner, which oversees implementation and enforcement of the act,[148] while Uganda's Data Protection and Privacy Act creates a National Information Technology Authority tasked with ensuring compliance with the act.[149]*

The data protection authority should be an **independent administrative authority responsible for ensuring all personal data, including health data, is processed in compliance with data sharing and protection principles.** The authority would authorize intercountry transfers of personal health data and could help set up mechanisms for cooperation with data protection authorities in other countries.

The national data protection authority should also **create systems of oversight to ensure accountability for appropriate health data sharing and protection**.

> EXAMPLE:
> *Kenya's Data Protection Act tasks the national data protection authority and the Office of the Data Protection Commissioner with establishing and maintaining a register of data controllers and data processors; promoting self-regulation among these controllers and processors; conducting assessments to ascertain whether information is processed according to the provisions of the Data Protection Act or other relevant laws; and promoting international cooperation to ensure each country's compliance with data protection obligations under international conventions and agreements.[150]*



The national data protection authority in each member state should **appoint a focal person on health data sharing and protection**. This individual should serve as the liaison between the data protection authority and the ministry of health as well as between the data protection authority and IGAD. Ministries of health should accordingly appoint a focal person to engage with the national data protection authority regarding implementation of health data sharing and protection measures.

When establishing the scope of responsibilities of the data protection authority, member states should take into account cases in which governance structures already exist and apply to some health data, such as personal data required for research. This is to ensure that the roles are sufficiently differentiated. For instance, Kenya's Data Protection Act provides an exception that allows lawful processing of personal data if the process is necessary for "historical, statistical, journalistic, literature and art or scientific research" purposes.[151]

Given that IGAD member states are in varying stages of developing and enacting national data protection regulations, **ministries of health in each member state should lead the development of national guidelines that will facilitate the adoption and implementation of the principles outlined in this regional policy**. In line with the implementation guide developed to support rollout of this policy, member states should develop a national implementation road map that will enhance accountability for how each country is integrating cross-border health data sharing and protection. Using the established national health sector coordinating mechanisms in each country, ministries of health should collaborate with relevant health and non-health sector stakeholders to improve cross-border sharing of health and health-related data in line with this policy. These coordinating structures, which may include existing technical working groups, should be used to mainstream the required data collection, analysis, and storage processes that support enhanced cross-border data sharing in the IGAD region. Implementation of cross-border health data sharing should exist at all levels, including subnational levels where health system leaders and implementors should be empowered to contribute to the implementation of the regional policy.

With support from IGAD, member states should continue to **strengthen their national health information management systems** to ensure improved data quality and timely sharing of agreed-upon health data across borders. Member states should also **prioritize advocacy and continued communication across all sectors** regarding the benefits of implementation of this regional policy. This advocacy will also support identification of opportunities to embed the principles of data sharing and data protection within other sectors that produce and collect health and health-related data, thereby increasing the available data for evidence-based decision-making.

At the regional level, IGAD has in place an institutional framework that is well suited to provide overall oversight and stewardship for the implementation of the Regional Health Data Sharing and Protection Policy. Along with this regional framework of governance, each member state should set up national implementation and enforcement mechanisms that will work together with regional bodies to coordinate.

OVERVIEW OF IGAD'S INSTITUTIONAL FRAMEWORK AND DATA SHARING STEWARDSHIP DUTIES

A ASSEMBLY OF HEADS OF STATE AND GOVERNMENT

The Assembly of Heads of State and Government is the supreme organ of IGAD.

B COUNCIL OF MINISTERS

The Council of Ministers (IGAD-CM), composed of the ministers of foreign affairs and one other focal minister designated by each member state, is the policy organ of IGAD to promote, monitor, coordinate, and harmonize initiatives to realize the objectives of IGAD. IGAD-CM may establish ad-hoc sectoral committees to deal with issues in their respective sectors in accordance with Article 10(3) of the agreement establishing IGAD.

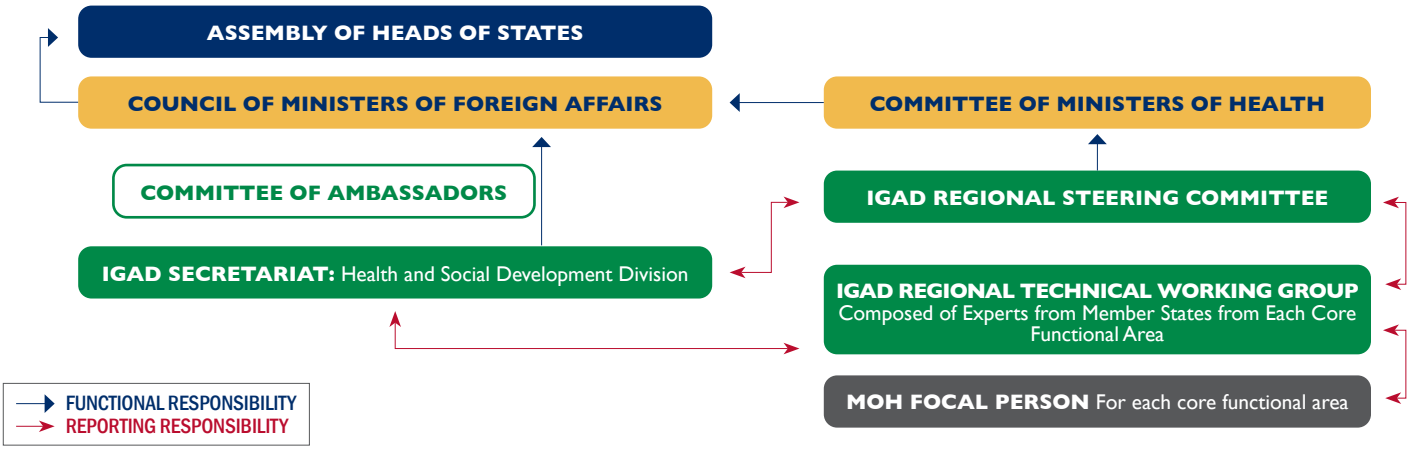
C COMMITTEE OF AMBASSADORS

The Committee of Ambassadors, comprising the ambassadors or plenipotentiaries of IGAD member states accredited to the country of IGAD's headquarters, advises and guides the executive secretary and promotes efforts to realize the work plans approved by the Council of Ministers.

D IGAD SECRETARIAT

The secretariat is the executive arm headed by an executive secretary appointed by the Assembly of Heads of State and Government. Besides Administrative and Finance, the secretariat has three operational divisions, namely for Economic Cooperation, Health and Social Development, Peace and Security, and Agriculture and Environment. Under the IGAD Health and Social Development division, the IGAD health desk will oversee the implementation of data sharing policies, as its mandate includes developing common strategies to control health problems at country borders; coordinating a regional health information system and exchange of information; promoting the improvement of health services at border areas; and monitoring the implementation of health protocols signed by IGAD.[152]

The **IGAD secretariat shall undertake work in collaboration with IGAD member states to harmonize national health data sharing and protection legislation and policies** and thereby promote seamless sharing of health data between the states. This harmonization support will include support to member states to identify focal points and appropriate structures in each country that will drive implementation of this regional policy.



With support from IGAD, member states will review existing national policies and laws to ensure that the domestication of this regional policy is aligned with existing national regulations and policies. Countries will also seek to use existing national and subnational structures to implement this policy to ensure operational efficiencies. In addition, IGAD shall advise member states on the format and procedure for the exchange of information between controllers and processors across the IGAD member countries as well as issue guidelines, recommendations, and best practices on intercountry exchanges of health data.

Given that several countries are members of more than one regional economic community (REC), member states will work with IGAD and other RECs to ensure that efforts toward data sharing and data protection are harmonized and synergies are created at the country level.

REFERENCES

1. Centers for Disease Control and Prevention, National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention, Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action, 2011, 72.{{COMMENT: Please note that, per Chicago style, the numbers at the start of each footnote should be formatted to be in line rather than superscript (in this example, 1. Centers for Disease Control}}
2. Institute of Medicine (US) Committee on Regional Health Data Networks, Health Data in the Information Age: Use, Disclosure, and Privacy, ed. Molla S. Donaldson and Kathleen N. Lohr, 1994, Sec.: Definitions, https://www.ncbi.nlm.nih.gov/books/NBK236546/.
3. Government of Kenya, "Data Protection Act, 2019," 2019, http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf; Government of Uganda, "The Data Protection and Privacy Act, 2019," 2019, https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf.
4. Ria Setyawati and Irena Audila, "Facing Cross Border: The Protection for Undertakings and Social Welfare in Indonesia" (Bandar Lampung, Indonesia: EAI, 2019), Sec.: Definitions (Cross-Border Cartel), https://doi.org/10.4108/eai.10-9-2019.2289430.
5. Helena Legido-Quigley et al., "Cross-Border Healthcare in the European Union: Clarifying Patients' Rights," BMJ 342 (January 17, 2011), https://doi.org/10.1136/bmj.d296.
6. Republic of Kenya, Ministry of Health, Kenya National EHealth Policy 2016–2030, 2016.
7. Intergovernmental Authority on Development (IGAD), "IGAD," accessed March 9, 2020, https://igad.int/.
8. European Union, "Art. 4 GDPR—Definitions," 2018, https://gdpr-info.eu/art-4-gdpr/.
9. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," 2010, Art. 1: Definitions, http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.
10. Merriam-Webster, "Misuse" (definition), 2019, https://www.merriam-webster.com/dictionary/misuse.
11. Team ObserveIT, "5 Examples of Data & Information Misuse," June 25, 2018, Sec.: What Is Data Misuse?, https://www.observeit.com/blog/importance-data-misuse-prevention-and-detection/.
12. Government of Kenya, "Privacy and Data Protection Policy and Bill," 2018, Appendix A: Definitions of Key Terms, http://jadili.ictpolicy.org/docs/privacy-and-data-protection-policy-and-bill-,2018.
13. European Union, "Art. 4 GDPR—Definitions."
14. European Union, "Art. 24 GDPR—Responsibility of the Controller," 2018, https://gdpr-info.eu/art-24-gdpr/.
15. International Organization for Migration, "IOM Data Protection Manual," 2010, Sec.: Glossary, https://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf.
16. European Commission, "What Are Data Protection Authorities (DPAs)?," accessed July 21, 2020, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en; European Union, "Art. 4 GDPR—Definitions," May 25, 2018.
17. Centers for Disease Control and Prevention, Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action, Appendix A: Glossary.
18. International Organization for Migration, "IOM Data Protection Manual," Sec.: Glossary.
19. Centers for Disease Control and Prevention, Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action, Appendix A: Glossary.
20. Government of Kenya, "Data Protection Act, 2019."
21. Government of Kenya.
22. Centers for Disease Control and Prevention, Appendix A: Glossary.
23. Tara Nutley and Heidi W. Reynolds, "Improving the Use of Health Data for Health System Strengthening," Global Health Action 6, no. 1 (December 1, 2013): 20001, https://doi.org/10.3402/gha.v6i0.20001.
24. Republic of Kenya, Ministry of Health, Kenya National EHealth Policy 2016–2030.
25. Vital Wave, Inc., "Digital REACH Initiative Roadmap," 2017, Sec.: Definitions of Terms, https://www.eahealth.org/sites/www.eahealth.org/files/content/attachments/2019-02-06/Digital-REACH-Initiative-Roadmap_20171205_custom_size_0.pdf.
26. Cambridge Dictionary, "Member state" (definition), accessed January 23, 2020, https://dictionary.cambridge.org/us/dictionary/english/member-state.

27. Cornell Law School, Legal Information Institute, "Natural person" (definition), accessed March 9, 2020, https://www.law.cornell.edu/wex/natural_person.
28. Cornell Law School, Legal Information Institute, "Artificial person" (definition), accessed March 9, 2020, https://www.law.cornell.edu/wex/artificial_person.
29. Lauren Spigel, Samuel Wambugu, and Christina Villella, MEASURE Evaluation's Knowledge Management team, "MHealth Data Security, Privacy, and Confidentiality: Guidelines for Program Implementers and Policymakers," 2018, https://www.measureevaluation.org/resources/publications/ms-17-125a.
30. European Union, "Art. 4 GDPR—Definitions," 2018, 4.
31. United Nations Development Group, "Data privacy, ethics and protection guidance note on big data for achievement of the 2030 agenda," 2017, https://undg.org/wpcontent/uploads/2017/11/UNDG_BigData_final_web.pdf.
32. UCL, "Anonymisation and Pseudonymisation," Data Protection, April 24, 2019, https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and.
33. European Union, "Chapter 3—Rights of the Data Subject," 2018, https://gdpr-info.eu/chapter-3/.
34. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS."
35. Spigel, Wambugu, and Villella, "MHealth Data Security, Privacy, and Confidentiality," Sec.: Glossary.
36. International Telecommunications Union, Publication Composition Service, "Data Protection: Southern African Development Community (SADC) Model Law," 2013, Pt. 1: Definitions, https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf.
37. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS."
38. Intergovernmental Authority on Development, "IGAD Regional Strategy Volume 2: Implementation Plan 2016–2020," January 2016, Sec.: Information and Documentation, https://igad.int/documents/6-igad-rs-implementationplan-final-v6/file.
39. Intergovernmental Authority on Development.
40. IGAD Regional Action through Data (RAD), "Recommendations of the Steering Committee Meeting," 2018.
41. World Health Organization, "Atlas of EHealth Country Profiles 2015: The Use of EHealth in Support of Universal Health Coverage," 2015, http://www.who.int/goe/publications/atlas_2015/en/.
42. RAD Consortium, "Regional Action through Data: Policy Analysis of International and East African Actors," 2018.
43. European Union, "Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," 1995, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5.
44. Government of Kenya, "Data Protection Act, 2019."
45. Government of Kenya.
46. Government of Kenya.
47. Government of Uganda, "The Data Protection and Privacy Bill, 2015," 2015, Pub. L. No. 32, https://www.nita.go.ug/sites/default/files/publications/Data%20Protection%20and%20Privacy%20Bill%202015%20-published_0.pdf.
48. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS."
49. International Telecommunications Union, "Data Protection: Southern African Development Community (SADC) Model Law."
50. African Union, "African Union Convention on Cyber Security and Personal Data Protection," June 27, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.
51. European Union, "General Data Protection Regulation (GDPR)," 2018, https://gdpr-info.eu/.
52. European Union.
53. International Organization for Migration, "IOM Data Protection Manual."
54. Australian Government, Department of the Prime Minister and Cabinet, "Best Practice Guide to Applying Data Sharing Principles," March 15, 2019, https://www.pmc.gov.au/sites/default/files/publications/data-sharing-principles-best-practice-guide-15-mar-2019.pdf.
55. African Union, "African Union Convention on Cyber Security and Personal Data Protection."
56. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS."
57. International Telecommunications Union, "Data Protection: Southern African Development Community (SADC) Model Law."
58. African Union, "The African Charter on Statistics," February 4, 2009, Chap. 2: Objectives, Art. 2(1), https://au.int/sites/default/files/treaties/36412-treaty-0037_-_african_charter_on_statistics_e.pdf.

59. International Organization for Migration, "IOM Data Protection Manual," Sec.: Glossary.
60. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS."
61. European Union, "Art. 4 GDPR—Definitions."
62. European Union, "Art. 24 GDPR—Responsibility of the Controller."
63. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Art. 23: Principles of Consent and Legitimacy.
64. European Union, "Art. 5 GDPR—Principles Relating to Processing of Personal Data," 2018, https://gdpr-info.eu/art-5-gdpr/.
65. Vital Wave, Inc., "Digital REACH Initiative Roadmap," Sec.: Harmonisation, Standards & Interoperability Workstreams.
66. Vital Wave, Inc., "Digital REACH Initiative Roadmap."
67. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS."
68. European Union, "Art. 5 GDPR—Principles Relating to Processing of Personal Data."
69. Australian Government, "Best Practice Guide to Applying Data Sharing Principles."
70. Chatham House, "A Guide to Sharing the Data and Benefits of Public Health Surveillance," 2017, https://www.chathamhouse.org/sites/default/files/publications/research/2017-05-25-data-sharing-guide.pdf.
71. ScienceDirect, "Data Quality Dimension—An Overview," accessed February 21, 2021, https://www.sciencedirect.com/topics/computer-science/data-quality-dimension.
72. ScienceDirect.
73. Global Research Collaboration for Infectious Disease Preparedness, "Principles for Data Sharing in Public Health Emergencies," March 30, 2017, Sec.: Quality, https://doi.org/10.6084/m9.figshare.4733590.v2.
74. Chatham House, "A Guide to Sharing the Data and Benefits of Public Health Surveillance."
75. Global Research Collaboration for Infectious Disease Preparedness.
76. Spigel, Wambugu, and Villella, "MHealth Data Security, Privacy, and Confidentiality."
77. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Art. 31: Exceptions.
78. International Organization for Migration, "IOM Data Protection Manual," Subsection: Forms of Consent.
79. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Art. 23: Principle of Consent and Legitimacy.
80. European Union, "Art. 5 GDPR—Principles Relating to Processing of Personal Data."
81. United Nations, "Multilateral International Covenant on Civil and Political Rights," n.d., https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf.
82. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Pt. 7: Formalities of Requests for Opinions and Authorizations.
83. Australian Government, "Best Practice Guide to Applying Data Sharing Principles."
84. European Union, "Art. 5 GDPR—Principles Relating to Processing of Personal Data," 5.
85. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Pt. 7: Formalities of Request for Opinions and Authorizations.
86. Spigel, Wambugu, and Villella, "MHealth Data Security, Privacy, and Confidentiality," Fig. 7: Steps to Mitigate Security Risks throughout the Data Life Cycle.
87. Australian Government, "Best Practice Guide to Applying Data Sharing Principles," Subsection: Training of Users.
88. United Nations, "Multilateral International Covenant on Civil and Political Rights."
89. Ann Cavoukian, "Privacy by design: The 7 foundational principles," 2009, 5.
90. Government of Kenya, "Data Protection Act, 2019."
91. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Pt. 25: Principle of Purpose, Relevance and Preservation.
92. Spigel, Wambugu, and Villella, "MHealth Data Security, Privacy, and Confidentiality," Col. 7: Steps to Mitigate Security Risks throughout the Data Life Cycle.

93. Government of Kenya, "Data Protection Act, 2019."
94. Government of Uganda, "The Data Protection and Privacy Act, 2019," accessed January 23, 2020, Pub. L. No. 32, https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf.
95. C. M. O'Keefe, S. Otorepec, M. Elliot, E. Mackey, and K. O'Hara, "The De-Identification Decision-Making Framework," 2017, CSIRO Reports EP173122 and EP175702, https://publications.csiro.au/rpr/download?pid=csiro:EP175702&dsid=DS1.
96. Australian Government, Department of the Prime Minister and Cabinet, "Issues Paper for Consultation: New Australian Government Data Sharing and Release Legislation," July 4, 2018, Subsection: Build Trust in Use of Public Sector Data, https://www.pmc.gov.au/sites/default/files/publications/australian-government-data-sharing-release-legislation_issues-paper.pdf.
97. World Bank, "Unique ID Numbers | Identification for Development," accessed March 25, 2021, https://id4d.worldbank.org/guide/unique-id-numbers.
98. World Bank.
99. Jembi Health Systems, "Health In Africa | Jembi Health Systems | South Africa," accessed March 25, 2021, https://www.jembi.org.
100. Privacy International, "Kenyan Court Ruling on Huduma Namba Identity System: The Good, the Bad and the Lessons," accessed March 25, 2021, http://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons.
101. Spigel, Wambugu, and Villella, "MHealth Data Security, Privacy, and Confidentiality," Table 5: Recommendations to Ensure Data Security throughout the Project Life Cycle.
102. European Union, "Chapter 4—Controller and Processor," 2018, Art. 33: Notification of a Personal Data Breach to the Supervisory Authority, https://gdpr-info.eu/chapter-4/.
103. Government of Kenya, "Data Protection Act, 2019."
104. Government of Uganda, "The Data Protection and Privacy Act, 2019."
105. European Union, "Chapter 5—Transfers of Personal Data to Third Countries or International Organisations," 2018, Art. 44: General Principle for Transfer, https://gdpr-info.eu/chapter-5/.
106. Spigel, Wambugu, and Villella, "MHealth Data Security, Privacy, and Confidentiality."
107. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Chap. VI: Rights of the Individual Whose Personal Data Are the Subject of Processing.
108. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS."
109. European Union, "Chapter 5—Transfers of Personal Data to Third Countries or International Organisations," Art. 45: Transfers on the Basis of an Adequacy Decision.
110. Spigel, Wambugu, and Villella, "MHealth Data Security, Privacy, and Confidentiality."
111. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Art. 36: Transfer of Personal Data to a Non-Member ECOWAS Country.
112. East African Community, Information Repository, "Draft EAC Legal Framework for Cyberlaws," November 2008, Subsection 2.5: Data Protection and Privacy, http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y.
113. East African Community, Subsection 2.1.1: General Provisions.
114. European Union, "Art. 45 GDPR—Transfers on the Basis of an Adequacy Decision," 2018, https://gdpr-info.eu/art-45-gdpr/.
115. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Art. 19: Responsibilities.
116. Economic Community of West African States, Art. 36: Transfer of Personal Data to a Non-Member ECOWAS Country.
117. Spigel, Wambugu, and Villella, "MHealth Data Security, Privacy, and Confidentiality," Fig. 7: Steps to Mitigate Security Risks throughout the Data Life Cycle.
118. European Data Protection Supervisor, "Accountability." Accessed September 9, 2021. https://edps.europa.eu/data-protection/our-work/subjects/accountability_en.
119. European Union, "Chapter 3—Rights of the Data Subject."
120. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Chap. VI: Rights of the Individual Whose Personal Data Are the Subject of Processing.
121. International Telecommunications Union, "Data Protection: Southern African Development Community (SADC) Model Law," Pt. VII: Rights of the Data Subject.

122. European Union, "Chapter 3—Rights of the Data Subject," Art. 13: Information to be Provided Where Personal Data Are Collected from the Data Subject.
123. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Art. 38: Rights to Information.
124. European Union, "Chapter 3—Rights of the Data Subject," Art. 13: Information to be Provided Where Personal Data Are Collected from the Data Subject.
125. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Art. 39: Rights of Access.
126. International Telecommunications Union, "Data Protection: Southern African Development Community (SADC) Model Law," Sec.: Right of Access.
127. Government of Kenya, "Data Protection Act, 2019."
128. European Union, "Chapter 3—Rights of the Data Subject," 2018, https://gdpr-info.eu/chapter-3/.
129. European Union, "Chapter 3—Rights of the Data Subject," Art. 17: Right to Erasure.
130. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Art. 41: Right to Rectification and Destruction.
131. International Telecommunications Union, "Data Protection: Southern African Development Community (SADC) Model Law," Sec.: Right of Rectification, Deletion, and Temporary Limitation of Access.
132. European Union, "Chapter 3—Rights of the Data Subject."
133. European Union, "Art. 21: Right to Object."
134. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Art. 40: Right to Object.
135. International Telecommunications Union, "Data Protection: Southern African Development Community (SADC) Model Law," Sec.: Right of Objection.
136. European Union, "Chapter 3—Rights of the Data Subject."
137. Government of Uganda, "The Data Protection and Privacy Act, 2019."
138. European Union, "Art. 23 GDPR—Restrictions," 2018, https://gdpr-info.eu/art-23-gdpr/.
139. Economic Community of West African States, "Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS," Chap. VII: Obligations of the Personal Data Controller.
140. UN HCHR, "CONFERENCE ROOM PAPER # 2," 2008, https://www.ohchr.org/Documents/Issues/Expression/ICCPR/Seminar2008/PaperCallamard.doc.
141. Omidyar Network, "Omidyar Network Unpacks Good ID: An Update to Our Point of View on Digital Identity | Omidyar Network," accessed July 21, 2020, https://www.omidyar.com/blog/omidyar-network-unpacks-good-id-update-our-point-view-digital-identity.
142. World Bank, "Principles | Identification for Development," accessed July 21, 2020, https://id4d.worldbank.org/principles.
143. Scottish Health Informatics Programme, "A Blueprint for Health Records Research in Scotland," August 12, 2011, http://www.scot-ship.ac.uk/sites/default/files/Reports/Appendix_6.pdf.
144. European Union, Art.4-Definitions, 2018.
145. European Union, Art. 24 GDPR – Responsibility of the controller."
146. European Union, "Chapter 4—Controller and Processor," Art. 28: Processor.
147. European Union, "Chapter 6 – Independent Supervisory Authorities" (2016), 6, https://gdpr-info.eu/chapter-6/.
148. Government of Kenya, "Data Protection Act, 2019."
149. Government of Uganda, The Data Protection and Privacy Act, 2019."
150. Government of Kenya, "Data Protection Act, 2019."
151. Government of Kenya, Sec. 30.1.
152. Intergovernmental Authority on Development, "IGAD-About IGAD," IGAD, 2020, https://igad.int/about-igad?start=5.