REPUBLIC OF UGANDA
MINISTRY OF HEALTH

THE UGANDA HEALTH DATA PROTECTION, PRIVACY AND CONFIDENTIALITY GUIDELINES

January 2023

DOCUMENT REVIEWS AND APPROVALS

Version	Owner	Author	Approver	Date of Approval *(MMDDYY)*
01	Ministry of Health	Division of Health Information Management	Top Management Committee	18.09.2024

TABLE OF CONTENTS

FOREWORD

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

However, the health sector must uphold the highest standards of data protection, privacy, and confidentiality through operationalising the Data Protection and Privacy Act 2019 within the sector. The Uganda Health Data Protection, Privacy, and Confidentiality Guidelines will serve as a cornerstone in ensuring the integrity and protection of health information in our nation.

In an era where digital technologies are revolutionising the way we collect, process, store, and utilise health data, a robust framework to safeguard sensitive information must be established. These guidelines provide comprehensive guidance to healthcare providers, policymakers, and stakeholders on best practices for protecting health data throughout its lifecycle.

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

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

Dr. Henry G. Mwebesa

DIRECTOR GENERAL HEALTH SERVICES

PREFACE

This document presents Uganda's Health Data Protection, Privacy, and Confidentiality Guidelines for the Health Sector. These guidelines are intended to standardize the implementation of health data protection, privacy and confidentiality across Uganda's health system. They are aligned with the Data Protection and Privacy Act 2019, Data Protection and Privacy Regulations 2021, National ICT Policy 2018, Health Information and Digital Health Strategic Plan 2020/2021-2024-2025, Ministry of Health Strategic Plan 2020/2021-2024-2025. The guidelines are also aligned with the Uganda Digital Health Enterprise Architecture, Standards and Knowledge Guidelines.

Health Information and supporting systems are critical assets for health service delivery. In Uganda like in many places, health data is faced with many privacy and confidentiality threats from a wide range of sources. Therefore, protecting the health data of Uganda's health system clients is of prime importance to the Ministry of Health. These guidelines aim to support all health stakeholders in the collection, transmission and storage of health data.

These guidelines will serve as a framework to ensure the protection of personal health data, secure information access, exchange, and storage as well as timely identification and addressing of vulnerabilities.

In addition, the guidelines will ensure that health data protection, privacy and confidentiality are observed by all health practitioners (including public and private) while handling health data (from collection, processing, storage and access). All health data stakeholders are called upon to embrace the use of these guidelines while handling any form of health data.

....

Dr. Sarah Byakika

Commissioner Health Services

Department of Planning, Financing and Policy

ACKNOWLEDGEMENT

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

I acknowledge and thank all development and implementing partners that provided financial and technical support for this process, specifically MUSPH/METS, HISP, IDI, CDC, The Technical Assistance Platform (TAP) and the University of Warwick. DHIM is grateful for all the support, sacrifice, and contributions that have been invested in the successful development of these guidelines.

Finally, the Ministry of Health is grateful to the Ministry of ICT&NG, NITA-U, Uganda Health Informatics Association, Makerere University Health Informatics Research Group and the Personal Data Protection Office (PDPO) and all those institutions and individuals who have not been specifically mentioned above, but who directly or indirectly contributed to the successful development and finalisation of the Uganda Health Data Protection, Privacy and Confidentiality Guidelines.

....

Mr. Paul Mbaka

Assistant Commissioner Health Services

Health Information Management

ABBREVIATIONS AND ACRONYMS

DHIM	Division of Health Information Management
HIIRE	Health Information Innovation and Research
ICT	Information Communication Technology
MOH	Ministry of Health
TWG	Technical Working Group
PDPO	Personal Data Protection Office

DEFINITION OF TERMS

Anonymization	Is an irreversible process of transforming or converting personal data to a form in which a data subject cannot be identified through any means reasonably.
Biometric Data	Personal data resulting from measurements and calculations relating to the physical, physiological, or behavioural characteristics of a natural person that allow or confirm the unique identification of that natural person, such as facial images or fingerprint data.
Confidentiality	The obligations of those who receive information are to respect the privacy interests of those to whom the data relates.
Consent	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the collection and processing of personal data relating to them.
Consent Artefact	A machine-readable document that specifies the parameters and scope of data access, sharing and use that a data subject consents to in any personal data-sharing transaction.
Consent Manager	A person who facilitates the consent process by providing tools and mechanisms for obtaining, managing, and documenting user consent in a transparent and user-friendly manner.
Data	Data means information which— a) Is processed using equipment operating automatically in response to instructions given for that purpose;

	b) Is recorded with the intention that it should be processed using such equipment; c) Is recorded as part of a relevant filing system or with the intention that it should be part of a relevant filing system; or d) Does not fall under paragraphs (a), (b), and (c). But forms part of an accessible record. A representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means.
Data Collector	A person or an entity that collects personal data.
Data Controller	A natural or legal person (e.g., an organization or other entity) who alone, jointly with other persons, in common with other persons, or as a statutory duty determines the purpose for and the manner in which data is processed or is to be processed.
Data Processor	A natural or legal person (e.g., an organisation or other entity) that processes personal data on behalf of the data controller.
Data Protection Officer	Is an individual employed by a data controller who understands and applies data protection regulations to the data control operations and serves as a liaison between the data controller and regulators.
Data subject	An individual from whom or in respect of whom personal information has been requested, collected, collated, processed, or stored.
De-identification	The process by which a data controller or data processor may remove or mask identifiers from personal data, or replace them with a

	fictitious name or code that is unique to a data subject but does not, on its own, directly identify the data subject.
Health Data	Personal data related to the physical or mental health of a natural person, including the provision of health care services that reveal information about their health status.
Natural persons	A living human being
Nominee	Is a natural person or legal entity who is selected or appointed by a data subject to act on their behalf in a specific capacity to access their personal data in the event of death or physical incapacity.
Personal data	Information about a person from which a person can be identified that is recorded in any form and includes data that relates to — a) The nationality, age, or marital status of a person; b) Education level or occupation of a person; c) An identification number, symbol or other particulars assigned to a person; d) Identity data; or e) Other information that is in possession of, or is likely to come into the possession of a data controller and includes an expression of opinion about the individual. Any information relating to an identified or identifiable natural person (i.e., a data subject).
Personal health identifier	A subset of "personal data", is the data that, alone or combined with other information could potentially identify a data subject and/or be used to distinguish one data subject from another; a

	personal health identifier could also be used to re-identify previously de-identified data and could include a data subject's demographic and location information, family and relationship information, and contact details.
Personally Identifiable Information	Any personal data that can be used to clearly identify an individual. Personally identifiable information includes names, physical and internet protocol addresses, financial information, login information , biometric identifiers, video footage, geographic location data, social media accounts, email addresses, and insurance identification number.
Privacy	An individual's right to control the acquisition, use, or disclosure of their personal information.
Protection	The process of protecting sensitive information from damage, loss, or corruption.
Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately so as to ensure that the personal data is not attributed to an identified or identifiable natural person.
Sensitive personal data	A subset of "personal data", means such personal information that consists of information relating to an individual's (i) password; (ii) financial information such as bank account, credit card, debit card, or other payment instrument details; (iii) physical, physiological, or mental health condition; (iv) sexual orientation; (v) political opinions, religious or philosophical beliefs, data revealing racial or

	ethnic origin, or trade union membership; (vi) medical records and history; (vii) biometric information; or (viii) details provided to entities providing services and processed or stored under lawful contract or otherwise provided that any information that is freely available or accessible in a public domain or made available under any applicable law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.
Third-party	A natural or legal person, public authority, agency, or body other than the data subject, data controller, or data processor, and a person who, under the direct authority of the data controller or data processor, is authorized to process personal data.

1.0 INTRODUCTION

The Ministry of Health recognises the need to harness data for improved health service ‘delivery, and it is in the process of digitising health service delivery in line with its Health Information and Digital Health Strategic Plan 2020/21 – 2024/25, Ministry of Health Strategic Plan 2020/21 – 2024/25, the National Development Plan III, and the Uganda Vision 2040, among others.

Digitisation of service delivery is recognised by the Government of Uganda as a key enabler for service optimisation. However, the Ministry of Health is cognisant of the fact that there is a need to adhere to the National Data Protection and Privacy Act 2019.

This document presents the Health Data Protection, Privacy, and Confidentiality Guidelines for Uganda that operationalises the Data Protection and Privacy Act 2019, and the Data Protection and Privacy Regulations 2021 within the health sector.

2.0 PURPOSE AND SCOPE

The guidelines seek to establish an effective, transparent, and accountable framework for managing health data protection, privacy, and confidentiality and ensuring compliance with the Data Protection and Privacy Act 2019.

These guidelines aim to ensure “Security and Privacy by Design” for the protection of personal data (both digital and paper-based) concerning the health of individuals living in the country. The guidelines shall set out the minimum standards for data protection, privacy, and confidentiality that should be followed throughout the health sector to ensure compliance with the Data Protection and Privacy Act 2019.

These guidelines are to be read along with, and not in contradiction to, any applicable law, or any instrument having the effect of any law; policies relating to information security and privacy, data retention, and data archiving; and any other policies or guidelines that may be notified from time to time.

OTHER LEGAL FRAMEWORKS

These guidelines are aligned with the following national documents adopted by the Government of Uganda; Computer Misuse Act 2011, the National Information Security Policy (framework) 2014, the Electronic Signatures Act 2011, the National Records and Archives Act 2001, the Access to Information Act (2005), and the Electronic Transactions Act 2011.

3.0 OBJECTIVES

The main objective of these guidelines is to provide guidance and establish a framework for the secure collection, processing, storage and use of personal and sensitive data within the health sector.

The specific objectives of these Guidelines include;

i. Protection of personal data, including personal health identifiers, within the jurisdiction of the national health care system by implementing adequate technical measures across the national health care system;
ii. Establish appropriate institutional mechanisms for auditing the data privacy, protection, and confidentiality controls, as needed, and support stakeholders and ecosystem partners to adopt the data protection principles established in these Guidelines;
iii. Establish that all eligible entities adhere to and comply with the applicable laws, rules, regulations, and any other standards about the protection and processing of personnel with in the health sector

4.0 DEVELOPMENT METHODOLOGY

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

4.1 HEALTH DATA TO BE PROTECTED

The personal data to be protected includes but not limited to;

1. Information about an individual for the provision of health services, research, or enforcement of the law. [1]
2. Information about payments or eligibility for healthcare concerning the individual.
3. A number, or particular symbol assigned to an individual to uniquely identify the individual for health purposes.
4. Information derived from the testing or examination of a body part or bodily substance, and identification of a person (e.g., a health professional) as a provider of healthcare to the individual.
5. Health data in various forms, including; electronic and paper-based data, pictures, audio, and videos.

5.0 HEALTH DATA MANAGEMENT COMPONENTS

This section of the document introduces health data management components to be protected under the Health Data Protection, Privacy, and Confidentiality Guidelines for Uganda.

5.1 DATA COLLECTION

All stakeholders involved with collecting and/ or capturing health information are required to:

a. Define the objective(s) for collecting and/ or capturing data [5] before information-gathering activities.
b. Define how the data shall be collected, transmitted, and stored.
c. Define the volume of data collected at any moment (quantity).
d. Ensure all proposed data to be collected and/ or captured, including tools, are approved by the data controller.
e. Obtain consent from the data subjects before data collection.
f. Have a data risk assessment before data collection.
g. Electronic data shall be collected per the MoH ICT Policy Guidelines

5.2 DATA PROCESSING

1. Data processing means any operation that is performed upon collected data by any means or otherwise, including:
    a. Organisation, adaptation or alteration of the information or data;
    b. Retrieval, consultation or use of the information or data
    c. Disclosure of the information by transmission, dissemination or otherwise making available, or;
    d. Alignment, combination, blocking, erasure, or destruction of the information or data
2. Before data processing, health data shall be classified using the following:
    a. Based on its sensitivity to disclosure, low-risk, medium-risk, and high-risk
    b. The criticality of information should always be classified through a risk assessment, i.e., obligatory and supplementary. The extent to which the information is essential for the ongoing provision of healthcare
    c. Based on time, it can be classified as current, future or historical
3. Data processing shall be conducted in alignment with the MoH ICT Policy Guidelines;

    a. Request to correct or delete personal data
    b. The data controller shall design a relevant form that shall be used to process any requests from data subjects.

5.3 DATA CORRECTION

a. A data subject shall, in writing, request the data controller to correct or delete their personal data which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or
b. Destroy or delete a record of personal data about the data subject held by the data controller that the data controller no longer has the authority to retain.
c. Upon receipt of the request, the data controller [18] considers the request and informs the data subject in writing of its decision within seven days after receipt of the request.
d. Where the data controller is satisfied [19] [20] with the request, the data controller shall comply.

e. Where the data controller cannot comply with the request, the data controller shall, in writing, inform the data subject of the rejection, the reasons for the rejection, and any action taken as a result of the request.

f. The manner of informing the data subject about the correction made shall be determined by the data controller, taking into consideration the correction made, the nature of the personal data, and the number of persons to whom the change has to be communicated.

5.4 PROCESSING PERSONAL DATA OUTSIDE UGANDA

a. A data collector, data processor [22], or data controller shall not process or store personal data outside Uganda unless such data collector, data processor or data controller seeks authorisation from the PDPO [23]

b. That the country outside Uganda where the personal data [24] is to be processed or stored has adequate measures in place for the protection of the personal data, at least equivalent to the protection provided for by the Data Protection and Privacy Act 2019.

5.5 DATA STORAGE

a. Health information shall be stored as guided by the MoH. The Division of Health Information Management (DHIM) shall be responsible for developing the SOPs and ensuring compliance of all health stakeholders (as stated in the MoH ICT Policy Guidelines, and the relevant Data Management Guidelines)

b. Minimize data risks by ensuring that user devices only access data required to perform approved business activities at any given time (as stated in the MoH ICT Policy Guidelines).

c. The use of privately owned devices to handle health data should conform to the Ministry of Health's ICT Policy Guidelines.

d. Digital Health Information shall be encrypted to protect it from unauthorised access and theft.

e. Electronic Data storage shall be conducted as detailed in the Ministry of Health's ICT Policy Guidelines.

f. All persons and entities collecting, processing and storing health data shall be registered by the PDPO.

g. A registry of third-party entities processing data on behalf of MoH shall be maintained at MoH. [17]

5.6 DATA RETENTION, ARCHIVAL AND DISPOSAL

a. All health data shall be retained for a minimum period of 5 (five) years from the date of creation before being archived. However, organizations shall establish their policies for the retention of health data based on legal requirements, industry standards, and operational needs while observing the minimum period for data retention. These policies shall outline specific retention periods for different types of health records, such as medical records, diagnostic test results, treatment plans, and billing information.

   The retention period shall also vary depending on the purpose for which the data was collected. For example, some data may need to be retained for a longer period for continuity of care, while other data may only be needed for a specific period for billing or research purposes. Organisations should assess the ongoing need for health data and establish appropriate retention periods based on its relevance and usefulness.

b. Ministry of Health and stakeholders handling sensitive patient health information for Ugandans shall only dispose of data in line with the Ministry of Public Service, and National Records and Archives Act 2001.

c. Patients shall have the right to request for deletion or destruction of their health data under certain circumstances, such as when the data is no longer needed for the purposes for which it was collected.

5.7 DATA SECURITY BREACHES

In case of a data security breach, the Ministry of Health ICT Policy Guidelines specifically the Incident Management Plan shall take effect and all incident management processes shall be followed and applied in reference to Section 11.2.

All data breaches shall be reported to the PDPO immediately after becoming aware of it

5.8 RIGHT TO ACCESS PERSONAL INFORMATION

Where the need arises, a data subject shall have to request access to personal information from the data controller who shall grant access after thorough verification. A request for access to personal information shall be made in a prescribed form or manner.

5.9 DATA ACCESS CONTROLS FOR THIRD PARTIES

Where there is a need to allow third-party access to the information processing facilities or personal health information, MOH or the relevant Data Controller shall carry out a risk assessment to identify any requirements for specific security controls. These controls shall include;

a. The legitimacy of the data requester must be ascertained.
b. The purpose for which the data is requested must be clear to the controller.
c. The request must be formal; in writing (either digital or paper)

5.10 DATA CLASSIFICATION

Data classification shall follow Section 8.0 of The Uganda Health Data Access, Sharing and Use Guidelines.

6.0 COMPLAINTS AND INVESTIGATIONS

6.1 COMPLAINT HANDLING

Any complaint related to health data protection, privacy, and confidentiality shall be reported to the person designated as the Data Protection Officer within the institution or the overall accountable person of the respective institution.

6.2 HEALTH INFORMATION EXCHANGE

Specific guidance on health information exchange can be found in the Uganda Digital Health Enterprise Architecture, Standards and Knowledge Guidelines, and Uganda Health Information Exchange and Interoperability Guidelines. The following guidelines shall be considered for health information exchanges.

a. Each HIE participant must comply with the Data Protection and Privacy Act 2019.
b. Each HIE participant must comply with Health Data Protection, Privacy, and Confidentiality Guidelines.
c. Each HIE participant must comply with Health Data Access, Sharing and Use Guidelines.
d. Each HIE participant shall report to their Organisation Management and the Personal Data Protection Office any breaches of confidentiality.

e. Established limitations shall be placed on the use and disclosure of protected health information.

f. Protected health information shall be secured by appropriate administrative, physical, and technical safeguards.

g. Each HIE participant shall report to the Ministry of Health any use of protected health information outside the established terms and conditions.

7.0 PRINCIPLES FOR DATA PROCESSING

These Guidelines shall ensure that data controllers and data processors adhere to the following principles while processing any personal data as permitted under the provisions of the applicable law(s):

a) Data processing must be lawful, fair, and transparent to the data subject. Data controllers shall take all necessary steps to maintain transparency in processing any personal data and shall make the following information available to the Ministry of Health as may be required:

   i. The classification (Section 5.2 (2)) of personal data generally collected and the manner of such collection;
   ii. The purposes for which the personal data are generally processed;
   iii. Any classification of personal data processed in exceptional situations, or for exceptional purposes that create a risk of significant harm.
   iv. The existence of, and the procedure for, the exercise of rights of data subjects and any related contact details for the same;
   v. The grievance redressal procedure;

b) In addition to the information specified above, the data controller shall also notify the data subject, from time to time, of important operations in the processing of any personal data related to the data subject. The information provided to the data subject shall be in an intelligible form, using clear and plain language.

c) Purpose limitation: All personal data collected and processed by data controllers should be for specific, clear, and legitimate purposes specified explicitly to the data subject in the privacy notice (Section 10.2) and consented to by the data subject. Further processing in the interest of public health archiving, scientific or historical research, or statistical purposes shall, in accordance with the relevant laws of the country such as the Data Protection and Privacy Act 2019, Uganda National Health Research Organisation Act, 2011, and Public Health Act among others.

d) Data minimization: Data collection and processing should be limited to as much data as absolutely necessary for the purposes specified. However, data minimization should not risk data quality or the quality of care. If data minimization risks the quality of care, it should be excluded from data processing.

e) Storage limitation: Personal data should be kept in a form that permits identification of data subjects for not longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in far as the personal data shall be processed solely in the interest of public health archiving, scientific or historical research, or statistical purposes, subject to implementation of the appropriate technical and organizational measures required by these Guidelines to safeguard the rights and freedoms of the data subject. Refer to Section 5.6 of these guidelines for further guidance on health data retention, archival and disposal.

f) Integrity and confidentiality: Data processing must be done in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical and organizational measures.

g) Privacy by Design: Data controllers shall consider data protection requirements as part of the design and implementation of their systems, services, products, and business processes. The Privacy Notice issued and the principles of Privacy by Design followed by the data controllers should align with these Guidelines and applicable law. Data controllers shall prepare a Privacy Notice containing the following information:

   i. Clear and easily accessible statements of their practices and policies;
   ii. Type(s) of personal or sensitive personal data collected.

iii. The purpose of collection and usage of such personal or sensitive personal data;

iv. Whether personal or sensitive personal data are being shared with other data controllers or data processors; and

v. Reasonable security practices and procedures used by the data controller to safeguard the personal or sensitive personal data that is being processed.

h) The Privacy Notice referred to in Section 10.2 shall be published on the website of the data controller. In addition, the data controller shall make available a Privacy by Design statement on its website containing the following information:

i. The managerial, organizational, and business practices, and technical systems designed to anticipate, identify, and avoid harm to the data subject;

ii. The obligations of data controllers;

iii. The technology used in the processing of personal data, in accordance with commercially accepted or certified standards;

iv. The protection of privacy throughout data processing from the point of collection to deletion of the personal data;

v. The processing of personal data in a transparent manner; and

vi. The fact that the interest of the data subject is accounted for at every stage of processing of personal data.

i) Choice and consent-driven sharing: Data controllers shall give data subjects a choice to opt in/opt out of the data sharing and processing and take their consent in accordance with Section 8.1 (a) of these Guidelines before accessing, sharing, or processing any of their personal data. This consent shall be free, informed, clear, and specific with respect to the purpose(s) identified in the privacy notice issued under Section 10.2 of these Guidelines. Insofar as the sharing or disclosure of any personal data is concerned, the technical design of the consent management framework should also ensure interoperability across the entire health information exchange ecosystem. The framework should be agnostic to applications, programming languages, and platforms.

j) Empowerment of data subjects: Data controllers should strengthen the rights of data subjects about their personal data. Data subjects shall enjoy rights as specified in Section 9.0 of these Guidelines.

k) Data quality: Data controllers shall take necessary steps so that the personal data that is processed is updated, complete, accurate, not misleading, and relevant to the purpose(s) for which it is processed. All personal data should be reliable and verifiable. However, the data controller shall not be responsible for the authenticity of the personal data supplied to them by the data subject. Personal data once created cannot be erased or amended without following the due process referred to in Section 5.3 and Section 5.6 of these Guidelines. All personal data must also be traceable to its collector unambiguously.

l) Accountability: Data controllers must be able to demonstrate compliance with the above principles (Section 7.0). They shall be accountable for complying with measures that give effect to the privacy principles while processing any personal data. However, the true ownership and control of the personal data shall remain with the data subjects.

m) Classification of personal data: Special provisions Section 5.2 (2) apply to the following types of personal data, whether or not they are related to health data:

   i. Information about an individual for the provision of health services, research, or enforcement of the law.

   ii. Information about payments or eligibility for healthcare concerning the individual.

   iii. A number or particular symbol assigned to an individual to uniquely identify the individual for health purposes.

   iv. Information derived from the testing or examination of a body part or bodily substance, and identification of a person (e.g., a health professional) as a provider of healthcare to the individual.

   v. Health data comes in various forms, including; electronic and paper-based data, pictures, audio and videos.

   vi. Health status.

   vii. Genetic or biometric data to uniquely identify a natural person;

   viii. Data concerning a natural person’s sexual activities or sexual orientation;

   ix. Political opinions, religious or philosophical beliefs, data revealing tribal or ethnic origin;

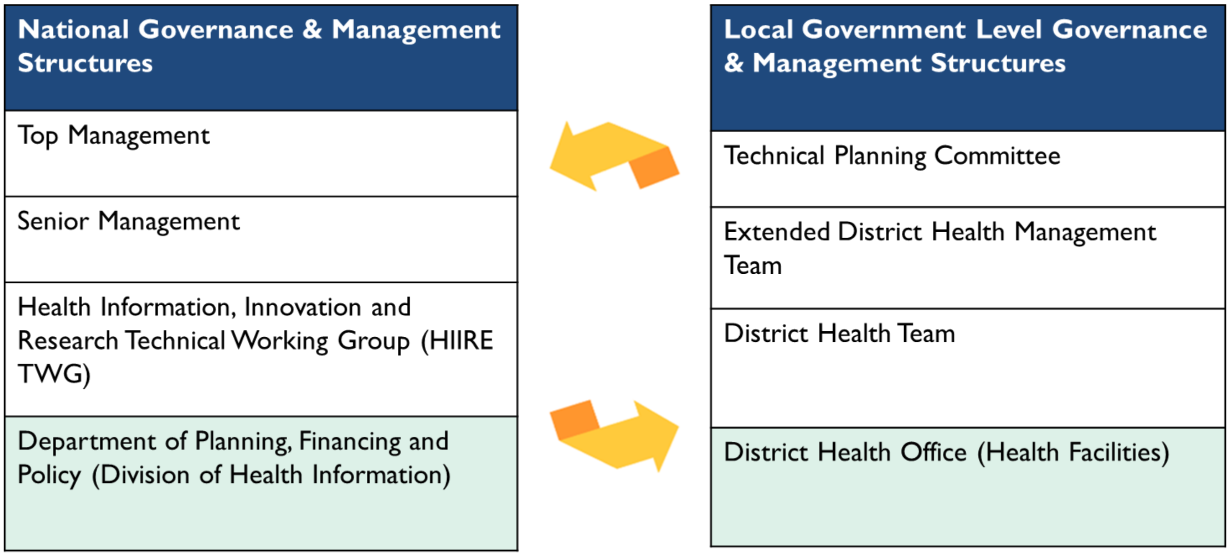
   x. Digital footprint created by users while accessing health data from an electronic system.

8.0 GOVERNANCE STRUCTURE

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

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

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



National Governance & Management Structures

- Top Management
- Senior Management
- Health Information, Innovation and Research Technical Working Group (HIIRE TWG)
- Department of Planning, Financing and Policy (Division of Health Information)

Local Government Level Governance & Management Structures

- Technical Planning Committee
- Extended District Health Management Team
- District Health Team
- District Health Office (Health Facilities)

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

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

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

The roles of the data controller, data collector, data processor, data protection officer, and data protection authority are described below;

8.1 DATA CONTROLLER

Technical and organizational measures: The data controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that data processing is performed in accordance with these Guidelines and any other applicable regulation. Appendix I provides a compliance checklist based on the Data Protection and Privacy Regulations 2021 compliance checklist. The data controller shall consider the nature, scope, context, and purposes of data processing as well as the risks and likelihood and severity of these risks as they relate to the rights and freedoms of data subjects to determine the technical and organizational measures. Those measures shall be reviewed and updated where necessary.

i. Taking into account the latest technological advancements, the cost of implementation, and the nature, scope, context, and purposes of data processing as well as the risks and likelihood and severity of these risks on the rights and freedoms of natural persons posed by the processing, the data controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, that are designed to implement data protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of these Guidelines and protect the rights of data subjects.

ii. The data controller shall implement appropriate technical and organizational measures (including physical measures) for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed. That obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage, and its accessibility. In particular, such measures shall ensure that by default personal data is not made accessible to an indefinite number of natural persons without the data subject's intervention.

iii. Code of conduct: Adherence to approved codes of conduct or approved certification mechanisms, as approved by the PDPO may be used as an element by which to demonstrate compliance of the data controller with the obligations set forth herein.

iv. Data breach notification: The data controller must notify the PDPO of any personal data breach immediately after becoming aware of it.

v. In the notification, the data controller must detail the nature of the breach, who has the most information on the breach, and the consequences and measures taken to address the breach.

vi. If the data breach poses a high risk to the rights and freedoms of data subjects, the data controller shall communicate the breach to the data subjects within 24 hours.

vii. Adherence to Guidelines requirements: Where data processing is to be carried out on behalf of a data controller, the data processor shall use only data processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that data processing shall meet the requirements of these Guidelines and thus protect the rights of the data subject.

8.2 DATA PROCESSOR

i. Adherence to Guidelines requirements: Data processing shall be carried out on behalf of the Data Controller. The data processor shall only implement appropriate technical and organizational measures after obtaining sufficient guarantees from the data controller and ensuring that data processing shall meet the requirements of these Guidelines and thus protect the rights of the data subject.

ii. Authorization: The data processor shall not engage another data processor without prior specific or general written authorization of the data controller. In the case of general written authorization, the data processor shall inform the data controller of any intended changes concerning the addition or replacement of other data processors, thereby allowing the data controller to object to such changes.

iii. Health Data sharing agreement: Health Data processing by a data processor shall be governed by a data sharing agreement as per the Uganda Health Data Access, Sharing and Use Guidelines and any other applicable law that is binding on the data processor with regard to the data controller and that sets out the subject matter and duration of the processing, the nature and purposes of the processing, the type of personal data, the categories of data subjects, and the obligations and rights of the data controller and the data processor.

iv. Data sharing agreement applicability: Where a data processor engages another data processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as described in Section 6.2 (iii) shall be imposed on that other data processor by way of a data sharing agreement or other legal contract under the applicable country law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing shall meet the requirements of these guidelines. Where that other data processor fails to fulfil its data protection obligations, the initial data processor shall remain fully liable to the data controller for the performance of that other data processor's obligations.

v. Adherence to code of conduct: Adherence of a data processor to an approved code of conduct or approved certification mechanisms, as approved by the PDPO, may be used as an element by which to demonstrate sufficient guarantees as referred to in Section 6.2 (i & iv).

vi. Legal basis: Without prejudice to an individual data-sharing agreement between the data controller and the data processor, the data-sharing agreement or other legal contracts in Section 6.2 (iii & iv) may be based, in whole or in part, on standard contractual clauses referred to in Section 6.2 (vii).

vii. Authority: The PDPO may lay down standard contractual clauses for the matters referred to in Section 6.2 (iii & iv) and in accordance with the governance procedures referred to in Section 6.2 (ii).

viii. Format: The data sharing agreement or other legal contracts referred to in Section 6.2, Bullets (iii) and (iv) shall be in writing, including in electronic format.

ix. Data processor as data controller: Without prejudice to Section 8.2 (ii–iv), if a data processor infringes these Guidelines by determining the purposes and means of processing, the data processor shall be considered to be a data controller in respect of that processing.

8.3 DATA PROTECTION OFFICER

a. Knowledge and expertise: The DPO shall be responsible for understanding data protection regulations and how they apply to the data controller, data processor and data collector; advising people in the organization about their responsibilities, conducting data protection training, conducting audits and monitoring of Guidelines/regulation compliance, and serving as a liaison with regulators.

b. Engagement: The data controller, data processor and data collector shall ensure that the DPO is involved, properly and in a timely manner, in all issues that relate to the protection of personal data.

c. Access: Data subjects may contact the DPO about all issues related to the processing of their personal data and to the exercise of their rights under these Guidelines.

d. Code of conduct: The DPO shall be bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Data Protection and Privacy Act 2019.

e. Conflict of interest: The DPO may fulfil other tasks and duties. The data controller, data processor, or data collector shall ensure that any such tasks and duties do not result in a conflict of interest.

f. Independence: The DPO shall be able to act independently, without any interference or influence from the data controller, data processor or data collector.

g. Key tasks: The DPO shall have at least the following tasks:

    i. Inform and advise the data controller, the data processor or the data collector of their obligations pursuant to these Guidelines and the Data Protection and Privacy Act 2019.

    ii. Educate and train employees who execute the Guidelines;

    iii. Monitor awareness-raising and training of staff involved in data processing operations;

    iv. Monitor compliance with these Guidelines, with Uganda data protection laws, and with the policies of the data controller or data processor or data collector in relation to the protection of personal data, including the assignment of responsibilities, and the related audits;

v. Provide advice where requested about the data protection impact assessment and to monitor its performance pursuant to Section 9 (iii);

vi. Guide any assessment of these Guidelines and initiate a Guidelines revision/update.

vii. Risk management: The DPO shall, in the performance of their tasks, have due regard for the risks associated with data processing operations, considering the nature, scope, context, and purposes of the data processing.

viii. Support: The data controller, data processor and data collector shall support the DPO in performing the tasks referred to in these Guidelines by providing the resources necessary to carry out those tasks, including access to personal data and data processing operations, and to maintain the data controller's expert knowledge.

ix. Supervision: The DPO shall directly report to the institutional management structures in place. He shall execute his roles/duties without interference from the data controller, the collector and the data processor as referenced in Data Protection and Privacy Regulations 2021. The DPO shall not be dismissed or penalized by the data controller or data processor or data collector for performing the tasks of a DPO.

9.0 RIGHTS OF DATA SUBJECTS

9.1 RIGHTS OF DATA SUBJECTS TO THEIR INFORMATION

Data subjects can request the following from data controllers:

a. Confirmation and access

Data subjects can obtain from data controllers the following information:

i. A confirmation as to whether the data controller has processed any personal data of the data subject;

ii. The personal data that has been processed or a summary of the same;

iii. A summary of processing activities carried out on such personal data; and

iv. Any information provided under the notice issued in accordance with Section 10.1 (a) of these Guidelines in relation to such processing.

b. The data controller shall provide the information under Section 9.1 (a) in a clear and concise manner that is comprehensible to a reasonable person.
c. The data subject shall also have the right to access, in one place, the identities of all the data controllers with whom their personal data has been shared and the categories of personal data that have been shared.
d. Correction and erasure:

   Data subjects can, with regard to the purposes for which their personal data are processed, rectify any inaccurate or misleading personal data, complete any incomplete personal data, and update any out-of-date personal data as outlined in Section 5.3 and Section 5.6. That is;

   i. A data subject shall have the right to initiate modification or correction of personal data stored in an electronic or paper system.
   ii. A data subject shall provide lawful justification and specify the type and data elements that should be modified or corrected. This justification shall be documented by the data controller for future reference

When data subjects request that their personal data be corrected or erased, the following rules shall apply:

i. The data may be corrected or erased if the storage of the personal data violates data protection principles or if the personal data is no longer necessary for the purpose for which it was processed.
ii. If the storage of personal data for a certain period of time is mandated by law, it cannot be erased.
iii. Data subjects can request the data controller to delete the uploaded personal data stored in their personal health record.
iv. Personal data can be blocked and restricted, rather than erased, in such instances where the law prohibits erasure as it would impair the legitimate interests of the data subject or entities that act as information providers (e.g., by collection, storing, or distributing health records).

v. Where erasure is not possible without disproportionate effort due to the specific type of storage, overwriting, or anonymization, then other methods (s) of removal of the personal data from live systems can be used.

vi. Erasure or destruction of any personal data shall be handled with the utmost care, in accordance with applicable laws, regulations, policies, standards, and guidelines, policies relating to information security, and guidelines relating to data retention and archival, as may be notified from time to time. Where data processors are erasing or destroying any personal data on behalf of the data controller, such erasure or destruction shall be in accordance with their contractual terms of service, and a notification of the erasure or destruction shall be required.

vii. Data erasure should be documented and must include information about the reason for data erasure, how it was erased/destroyed, when, and by whom.

e. Restriction or objection to disclosure: Subject to applicable law, data subjects can restrict or object to the disclosure of their personal data by the data controller.

f. Automated individual decision-making: Data subjects shall have the right to be informed in case a decision to be based solely on automated processing, including profiling, would produce legal effects concerning them or that similarly significantly affect them.

g. Data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning them or that similarly significantly affects them.

h. Section 9.1 shall not apply if the decision:

i. Is necessary for the entering into, or performance of, a contract between the data subject and data controller;

ii. Is authorised by a law to which the data controller is subject, and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or

iii. Is based on the data subject’s explicit consent (Section 8.1 (a)).

9.2 GENERAL CONDITIONS FOR SUBMITTING REQUESTS

a. All requests under Section 9.1 above shall be made by the data subject or a legally acceptable representative in writing, either electronically or physically on paper, to the designated officer of the data controller (referred to as a DPO),

b. The request shall be made with the necessary information in regard to the identity of the data subject, and the data controller shall acknowledge receipt of such request. All requests shall be addressed by the data controller within five (5) working days and in compliance with applicable laws, regulations, and these Guidelines.

c. In the event that any request for correction, completion, update, or erasure of any personal data is accepted by the data controller, such a data controller shall take the necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, update, or erasure, particularly where such action may have an impact on the rights and interests of the data subject or decisions made regarding them. The data controller shall also notify the data subject once the relevant personal data has been corrected, completed, updated, or erased within five (5) working days after the action of the request.

d. In the event that any request for correction, completion, update, or erasure of personal data is rejected, the data controller shall provide to the data subject the reasons, in writing, for such refusal within five (5) working days. If the data subject is not satisfied with such reasons, they may require that the data controller take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data subject.

e. In the event of the death of the data subject, the nominee of the data subject may have access to the personal data of the data subject only if such access by such person was specifically consented to by the data subject. If the deceased data subject did not consent, access shall be denied to those who request the personal data of the deceased data subject.

f. The data controller shall not impose any restrictions on the method or channel of raising requests by data subjects under Section 9.1 above.

g. The data controller shall maintain records of all requests received under Section 9.1 above, irrespective of their fulfilment status.

h. Data corrections and modifications should be subject to strict oversight. A request should be lawful and valid. If the modification is clinical, it should be reviewed by a clinician to ensure the correction being requested is reasonable and appropriate. If the correction is nonclinical (e.g., demographic information), there shall be a policy or process for permitting the correction without the oversight requirements. The correction should also be documented as to why, how, when, and by whom the data was corrected.

10. CONSENT FRAMEWORK

Data controllers can collect personal data, which shall be limited as specified in this section of the Guidelines.

Consent principles: The consent framework under these Guidelines incorporates the following principles in relation to the processing of personal data by data controllers:

a. Data subjects should own their personal data based on the data subjects' rights and determine how their data can be shared and used.
b. Specifically, in the case of electronic consent, data controllers should make use of appropriate technological means to prevent security breaches and to guarantee the integrity of access permissions given by data subjects. Such technological means must conform with the Uganda Data Protection and Privacy Act 2019 and other applicable international standards, as may be notified for the implementation of technical and organizational security measures from time to time.

10.1 CONSENT FOR DATA COLLECTION AND PROCESSING

a. Data controllers can collect or process personal data only with the consent of the data subject or other valid justifications for processing data, except when data sharing does not require the consent of the data subject, as referenced in **Data Protection and Privacy Act 2019 Part III Section 7B I-III**. It is the responsibility of the data controller to ensure that the consent given by the data subject is valid. The consent of the data subject shall be considered valid only if the data controller is able to demonstrate that the data subject consented to the processing of their personal data, and the consent is:
    i. Free from coercion, with regard to whether it complies with the standards set out under the Data Protection and Privacy Act 2019;

ii. Informed, with regard to whether the data subject has been provided with the necessary information by way of notice, as set out in Section 8 (a, b) of these Guidelines;

iii. Specific, where the data subject can give consent for the processing of their personal data for a particular purpose;

iv. Clearly given; a specific, informed and unambiguous indication of the data subject's wish which he or she, by a statement or by clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her; and

v. Capable of being withdrawn at any time, and the ease of such withdrawal is comparable to the ease with which consent may be given.

b. The purposes for the collection or processing of personal data shall be limited to those that may be specified by the PDPO and such purposes shall be related to the health of an individual or maybe such other incidental purposes that a data subject can reasonably expect for the purpose, context, and circumstances in which the personal data was collected or processed.

c. In addition to the conditions mentioned in Section 8.1 (a) of these Guidelines, the consent of a data subject with respect to the collection or processing of any personal or sensitive personal data shall be obtained only after informing the data subject of the purpose of the data processing and any processing that is likely to cause significant harm to the data subject.

10.2 PRIVACY NOTICE FOR THE COLLECTION OR PROCESSING OF PERSONAL DATA

a. All data controllers must give a clear and conspicuous Privacy Notice (Appendix II) to data subjects:

i. Prior to the collection of personal data from the data subject;

ii. At the time the data controller changes its privacy policies or procedures; and

iii. Prior to the collection or further processing of personal data of the data subject for any new or previously unidentified purpose.

b. Any entity collecting health data shall ensure that a Privacy Notice is displayed within their premises, particularly at service points.

c. It is clarified that for the purpose of Section 8.1,(a) above, all data controllers must obtain fresh consent from data subjects in accordance with the consent framework of these Guidelines.

d. The privacy notice shall contain the following information:

    i. The extent to which the personal data is to be processed, such as

    - Data controller sharing data with data processor for joint purposes,
    - Data controller sharing data with data processor for use by the data processor, and
    - Data controller using data for its own purposes;

    ii. The nature and categories of personal data being collected by the data controller;

    iii. The methods or mechanisms by which the personal data is collected by the data controller;

    iv. The identity and contact details of the data controller collecting the personal data;

    v. The right of the data subject to withdraw their consent, and the procedure for such withdrawal;

    vi. The individuals or entities along with their contact details, including other data controllers or data processors, with whom personal data may be shared, if applicable;

    vii. The period of time for which the personal data shall be retained, or where the period of retention is not known, then the criteria for determining such period;

    viii. The existence of and the procedure for the exercise of rights of the data subject as referred to in Section 7 of these Guidelines; and

    ix. The mechanism by which a data subject may contact the data controller in relation to complaints, inquiries, and clarifications regarding the policies, practices, and procedures employed in the collection, storage, transmission, or any other aspect of processing of personal data.

e. The privacy notice shall be clear, concise, and easily comprehensible to a reasonable person and shall be available in as many languages in which the services of the data controller are intended to be provided.

10.2.1 METHOD OF OBTAINING CONSENT

a. The consent of the data subject, as referred to in Sections 10.0 and 9.0 of these Guidelines, for collection or further processing of personal data, may be obtained electronically or physically on paper, either directly from the data subject or through a consent manager, as the case may be. Where the consent is received physically on paper, then such consent may be converted to electronic format by the consent manager or the data controller.

b. Where consent is obtained through a consent manager as set out above, then such consent manager shall:

   i. Not access, process, or store, in any manner whatsoever, the personal data shared with any data controller pursuant to any consent obtained through such consent manager;

   ii. Maintain a record of all consents shared and revoked, as the case may be, and maintain a log of consents/consent transactions in a manner that enables the audit and review of any use of personal data.

   iii. Where the data subject has revoked their consent, it shall be the duty of the consent manager to notify the data controller of such revocation, as applicable.

c. It is clarified that electronic consent is the digital equivalent of a physical letter of permission given by the data subject which, when presented, allows the consent manager or data controller to collect the personal data or further process the personal data that has already been collected from the data subject for a particular purpose, as the case may be

d. Insofar as further processing of personal data pursuant to Section 10.1 (i), (ii), and (iv) above is concerned, if such processing is done through electronic consent, then a consent artefact shall be generated to initiate the sharing of personal data. If the data subject provides consent for data access and sharing that takes place between a data controller and data processor, the consent artefact shall then be shared with the data controller and data processor through the consent manager.

e. Subject to the provisions of this Guideline and the Data Protection and Privacy Act 2019, guidelines and technical specifications may be set out by the PDPO in relation to consent obtained by data controllers for the collection and further processing of personal data of data subjects.

10.3 PROCESSING PERSONAL DATA PERTAINING TO A CHILD

a. The data controller(s) should obtain the consent of the parent or guardian of a child prior to processing the child's personal data.

b. A valid proof of relationship and proof of identity of the parent or guardian must be submitted to the data controller in order to verify the consent of the parent or guardian for processing the personal data of the child as set out in Section 10.3, (a) above.

c. Under the following situations, the child shall provide assent, and the parent shall not be the minor's personal representative under these Guidelines. These situations are:

   i. When the minor is the one who assents to care and the consent of the parent is not required under the Data Protection and Privacy Act 2019 or other applicable laws;

   ii. When the minor obtains care at the direction of a court or a person appointed by the court; or

   iii. when and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship. For example, a child can restrict a parent's access to their sexual health data according to the country law determining the age of medical consent for the child.

d. Even under the above exceptional situations (Section 10.3, (c), the parent may have access to the medical records of the minor when the Data Protection and Privacy Act 2019 or other applicable law requires or permits such parental access. Parental access would be denied when the Data Protection and Privacy Act 2019 or other law prohibits such access. If the Data Protection and Privacy Act 2019 or other applicable law is silent on a parent’s right of access in these cases, the licensed healthcare provider may exercise their professional judgement to the extent allowed by law to grant or deny parental access to the minor’s medical information. Finally, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in their professional judgment, that the child has been or may be subjected to domestic violence, abuse, or neglect, or that treating the parent as the child’s personal representative could endanger the child.

e. Data controller(s) shall not process the personal data of a child in a manner that is likely to harm the child.

f. Data controller(s) should ensure that the processing of the personal data of a child takes place only in such a manner that is in the best interests of the child.

10.4 PROCESSING PERSONAL DATA OF SUBJECTS WHO ARE SERIOUSLY ILL OR MENTALLY INCAPACITATED

Processing personal data of data subjects who are seriously ill or mentally incapacitated or in response to a life-threatening or severely health-threatening medical emergency:

a. When it is necessary to collect data from a seriously ill or mentally incapacitated subject, or in response to a life-threatening or severely health-threatening medical emergency a nominee shall represent the data subject until the subject becomes able to give consent.

b. At the time a data subject opts to participate in the data collection and processing, such data subject should name a nominee;

c. The nominee referred to in Section 10.4, (a) above shall be authorized to give valid consent on behalf of the data subject in the event the data subject becomes seriously ill or mentally incapacitated, or where the data subject is facing a life-threatening or severely health-threatening medical emergency and is unable to give valid consent.

d. In the event that the data subject has not named a nominee under Section 10.4 (a) above, then any adult family member of the data subject can give valid consent on behalf of the data subject.

e. In the event that there is no family member or nominee, an authorized person may consent on behalf of the data subject.

f. In the event that the data subject has named a nominee under Section 10.4 (a) but the nominee is unable to give consent for any reason, then the health care professional can use their best judgment until such nominee, family member, or data subject is able to give consent.

g. Consent can be given by a family member of the data subject, as set out in Section 10.4 (d) above, only where there is proof of relationship with the data subject.

11. DATA SECURITY, IMPACT ASSESSMENT, AND AUDIT

11.1 ADEQUATE SECURITY PRACTICES AND PROCEDURES

i. Data controllers shall implement such security practices and standards and have a comprehensive documented information security program and information security policy(ies)/guidelines that contain managerial, technical, operational, and physical security control measures that are commensurate with the data/information assets being protected by them (Appendix III) both in paper and electronic format. These security practices, standards, and policies shall be reviewed periodically.

ii. In the event of a data/information security breach, data controllers shall be required to demonstrate, as and when called upon to do so, to the PDPO and the Ministry of Health, that they have implemented security control measures as per their documented information security program and information security policies.

iii. Data controllers shall implement necessary security safeguards, including the use of de-identification and encryption methods, to protect the integrity of the personal data collected and to prevent the misuse of, unauthorized access to, modification of, disclosure of, or destruction of personal data. The necessary safeguards shall factor in the nature, scope, and purpose of processing the personal data, the risks associated with such processing, and the likelihood and severity of harm that may result from such processing. Data controllers shall undertake a review of their security safeguards periodically and take corrective measures accordingly.

iv. Data controllers shall implement the Uganda Digital Health Enterprise Architecture, Standards and Knowledge Guidelines as well as any other standards as may apply to them. Several relevant resources (e.g., International Organization for Standardization, US National Institute of Standards and Technology, and others) are included in these Guideline's bibliography that might be applicable for adequately securing, risk assessing, and implementing the data controller's infrastructure. Appendix IV shows how to assess and improve cybersecurity maturity.

v. As permitted under the provisions Data Protection and Privacy Act 2019, the standards in relation to security practices and procedures mentioned above may be certified or audited on a regular basis through an independent auditor duly approved by the Personal

Data Protection Office. This audit shall be carried out by the auditor at least once a year or when the data controller undertakes a significant upgrade of its processes, computer resources, or systems.

vi. If and when an entity is implementing or involved in the national health care system and is acting as a data controller in this regard, the DPO shall undertake a periodic review of the entity's security safeguards and take appropriate measures to update such safeguards, if required.

vii. Any person having access to health data shall be subjected to mandatory training once a year or access to head data systems shall be automatically revoked.

11.2 DATA MANAGEMENT BY DATA PROCESSORS

i. The data controller should conduct appropriate due diligence covering data privacy and security before engaging with any data processor.

ii. The data controller may not engage, appoint, use, or involve a data processor to process personal data on its behalf without a contract entered into by the data controller and such data processor.

iii. The data controller shall require its data processors to execute confidentiality agreements and nondisclosure agreements covering data protection and privacy responsibilities. Such agreements shall be reviewed, updated, and renewed periodically. The data controller may require that the confidentiality requirements under such agreements continue for a specified period even after the contractual period ends.

iv. Subject to the Data Protection and Privacy Act 2019, the agreements referred to in Section 11.2 (iii) shall align with these Guidelines. These agreements shall ensure that data processors adhere to the same level of data protection that is adhered to by the data controller.

v. The data controller shall require its data processors to limit their access only to the personal data necessary for the fulfilment of their employment/contractual duties and for public health, research, and statistical purposes based on a "need-to-know" principle, as the case may be.

vi. The data processor and any employee of the data controller shall only process personal data in accordance with the instructions of the data controller and treat it confidentially.

vii. The data processor may not engage, appoint, use, or involve another data processor in processing on its behalf, except with the authorization of the data controller and unless permitted in the contract referred to in Section 9.2 (ii) above.

viii. The data controller shall ensure that training and awareness materials around data protection and privacy are developed for its employees and data processors. Role-based training for individuals or teams that consider the nature of the processing and their roles shall be developed. Data privacy training and awareness programs shall be conducted on a periodic basis (at a minimum, annually) for all employees and data processors. Attendance records for such training shall be maintained for documentation and audit purposes.

11.3 DATA PROTECTION IMPACT ASSESSMENT

i. The data controller shall carry out a data protection impact assessment before it undertakes any processing involving new technologies or any other processing that carries a risk of significant harm to data subjects.

ii. The data protection impact assessment shall contain, among other things, a detailed description of the proposed processing operation, the purpose(s) of the processing, the nature of personal data being processed, an assessment of the potential harm, and measures for managing, minimizing, mitigating, or removing such risk of harm.

iii. The data controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Section 11.3 (i–ii) indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

11.4 RECORDS MAINTAINANCE

i. Data controllers shall maintain accurate and up-to-date records to document the important operations in the data life cycle, including collection, transfer, and erasure of personal data. These records shall cover the following:

a. Details of the ecosystem partners;

b. Purposes of the processing;

c. Description of the categories of data subjects;

d. Description of the categories of personal and sensitive personal data; and

e. Categories of recipients to whom the personal data is disclosed/transferred, including to data processors.

In addition to the records referred to in Section 11.4, (i) and elsewhere in these Guidelines, data controllers shall also maintain accurate and up-to-date records of the periodic review of security safeguards conducted under Section 11.1, data protection impact assessments conducted under Section 11.3, and requests received under Section 9.0 of these Guidelines.

Audit

i. Data controllers should maintain a strict audit trail of all processing of any personal data, at all times. This is the record of how personal data is processed by the data controller and should be maintained in a manner that enables the audit and review of any use of personal data.

ii. Data controllers should ensure that periodic audits of their data processors are conducted by third parties in accordance with relevant standards and certifications, as may be specified by the PDPO, to verify that such data processors process all personal data appropriately in compliance with all privacy notices, contracts/confidentiality agreements, these Guidelines, and any policy relating to information security as may be notified from time to time.

iii. If the data controller decides to update any personal data in accordance with Section 9.0 of these Guidelines, then the original personal data and an audit trail of the change shall be made available to the data subject. However, the updated personal data with a new version number shall be considered active.

12. DATA SHARING OBLIGATIONS

The data sharing obligations described in these Guidelines are an extension of the Uganda Health Data Access, Sharing and Use Guidelines and a Data Processing Agreement (Appendix V).

12.1 DATA CONTROLLERS SHARING PERSONAL DATA

i. Any personal data processed by a data controller may be shared with a data processor in response to a request made by such data processor for personal data pertaining to the data subject, only where consent of the data subject is obtained in accordance with Section 10. Consent framework, (a,b) of these Guidelines.

ii. Where a data processor makes a request to access any personal data under Section 12.1 (i), above, the data controller shall verify the constituents shared with it, including whether such consent has been revoked by the data subject. Where the consent is valid, it shall share such data with the data processor strictly in accordance with Section 10, (a,b) of these Guidelines.

iii. A data controller shall maintain a record of all consent obtained under these Guidelines, pursuant to which personal data has been shared by such data controller under these Guidelines in a manner that enables the audit and review of such data sharing.

iv. Where the data subject has provided their consent for the sharing of their personal data under these Guidelines, it shall not be used, disclosed, or shared by the data controller or any data processor in any other manner, or for any other purpose, except as provided in Section 10, (a,b) of these Guidelines.

v. A data controller should comply with permissible data-sharing scenarios outlined in the Uganda Health Data Access, Sharing and Use Guidelines, which does require data subject consent and complies with the legal justifications for data sharing outlined in Section 12.4 of these Guidelines. For example, data sharing between health care providers for treatment purposes should not require consent of data subjects and complies with Section 12.4 (iv) (vital interests of the data subject)

12.2 DATA CONTROLLERS SHARING DE-IDENTIFIED OR ANONYMIZED DATA

i. Data controllers may make anonymized or de-identified data in an aggregated form available as per the procedure set out in Section 12.2 (ii) to facilitate health and clinical research, academic research, archiving, statistical analysis, policy formulation, development and promotion of diagnostic solutions, and such other purposes as may be specified by the PDPO.

ii. The PDPO shall set out a procedure through which any entity seeking access to anonymized or de-identified data under these Guidelines shall be required to provide relevant information such as its name, purpose of use, and nodal person of contact. Subject to approval being granted under this procedure, the anonymized or de-identified data under these Guidelines shall be made available to such entity on such terms as may be stipulated herein.

iii. Any entity that is provided access to de-identified or anonymized data shall not, knowingly or unknowingly, take any action that has the effect of re-identifying any data subject or of causing such data to no longer be anonymized.

iv. The data controller that is undertaking to anonymize or de-identify data under these Guidelines shall be responsible for ensuring compliance with the procedure for such anonymization or de-identification as set out in these Guidelines under Section 12.2 and any noncompliance shall be dealt with as per Section 13.4.

v. The de-identification or anonymization of data by a data controller shall be done in accordance with technical processes and anonymization protocols that may be specified by the PDPO or the organisation ICT policy. The data controller should protect an anonymized database in the same way that it protects a database with personally identifiable information.

vi. The technical processes and anonymization protocols referred to in Section 12.2, (v) shall be periodically reviewed by the PDPO, and such review shall have regard to the nature and sensitivity of the data being processed, the risks of re-identification of data subjects, and the robustness of the anonymization protocols.

vii. Any attempt to re-identify individuals or to generate information (e.g., facial images or comparable representations) that could allow the identities of data subjects to be readily ascertained should be strictly prohibited (and subject to penalty) except where expressly authorized by law. Reasonable steps should be taken to prevent the identity of data subjects being leaked or determined through indirect means such as metadata, website URLs, and email subject lines .

12.3 RESTRICTIONS ON SHARING, CIRCULATING, OR PUBLISHING OF PERSONAL DATA

a. Any personal data of the data subject shall not be published, displayed, or posted publicly by any person or entity unless permitted by any other law.

b. A database or record of any data that has been processed under these Guidelines shall not be made public, unless such database or record is in an anonymized/de-identified and aggregated form and is processed in accordance with the terms specified in Section 12.2, (i) of these Guidelines.

12.4 LEGAL GROUNDS FOR PROCESSING PERSONAL DATA

The processing of personal data (Section7.0) is permitted under one or more of the following legal grounds:

i. Explicit consent (Section 10, (a,b)): the explicit consent of a patient must be freely given and comes with an obligation to not exceed the intent of the consent, so should be considered carefully.

ii. Performing a contract: a data controller may be able to process data for performing a contract (e.g., a company is allowed to process personal data for salary processing and a care provider may be able to exchange data with payers for fulfilling insurance contracts).

iii. Legal obligations: a data controller may be required to process the data to comply with legal obligations (e.g., reporting to authorities in a legal obligation).

iv. Vital interests of the data subject: the vital interests of the data subject may present a lawful justification for data processing (e.g., in case of a public health emergency or medical emergency scenario).

v. Public interest: public interest in the area of public health (e.g., protecting against serious infectious diseases such as HIV/AIDS and tuberculosis or ensuring high standards of quality and safety for health care, medicinal products, and medical devices) on the basis of Public Health Act 1935, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject. Public interest shall also include use of personal data for public health archiving, scientific or historical research, or statistical purposes. Processing of data for public health interest shall not include processing of personal data for other purposes by third parties, such as employers or insurance and banking companies.

vi. Legitimate interests, where these interests do not conflict with data subject rights or other protections: legitimate interests can be claimed but they must be justified (i.e., the interests must be confirmed as legitimate); for example, a pharmacy claiming that they have a legitimate interest to sell patient diagnosis data to maintain profit levels may not be claimed as a legitimate interest.

vii. If a processing activity or purpose does not fit into any of the legal justifications described above, the data processing may be considered unlawful.

13. GRIEVANCE REDRESSAL, INCIDENT MANAGEMENT, AND GUIDELINES COMPLIANCE

13.1 GRIEVANCE REDRESSAL

i. Data subject(s) with inquiries and questions about the processing of their personal data may approach a designated officer of the data controller (i.e., data protection officer) in writing, either through email or any other electronic means or physically on paper, as may be specified. The details of the DPO shall be provided on the official notice board / website/ approved platform of the data controller along with the format and process for filing inquiries/questions. Where feasible, the data controller may designate the DPO as the grievance redressal officer mentioned in Section 13.1, (ii) below.

ii. A complaint can be made by the data subject regarding any contravention of these Guidelines that has caused or is likely to cause harm to such data subject. The data controller shall have in place procedures and effective mechanisms to redress the grievances of data subjects efficiently and in a speedy manner. For this, the data controller shall designate a grievance redressal officer and publish their name and contact details on its website or on the official notice board. The grievance redressal officer shall redress the grievances of the data subject expeditiously but within one month from the date of receipt of the grievance. Acknowledgment of receipt of a grievance shall be provided to the data subject within 7 working days.

iii. In the event that a complaint is not resolved by the grievance redressal officer of the data controller as referred to under Section 13.1 (ii) above, the data subject shall be notified and the matter may be referred to the PDPO in writing, or through email or any other electronic means provided under the grievance portal of PDPO website (https://www.pdpo.go.ug/file-complaint).

13.2 PERSONAL DATA BREACH AND INCIDENT MANAGEMENT

To address data security breaches, the following shall be undertaken:

i. The data controller shall formulate and implement a personal data breach management procedure, which shall be publicly displayed. The data controller shall also ensure that any instance of noncompliance with the provisions of these Guidelines, or any instance of unauthorized or accidental disclosure, acquisition, sharing, use, alteration, destruction of, or loss of access to personal data that compromises the confidentiality, integrity, or availability of personal data to a data subject is promptly notified to relevant entities as required by the Data Protection and Privacy Act 2019.

ii. The data controller shall also notify any incidents referred to in Section 13.2, (i), and the actions taken pursuant to such incidents, to the PDPO in a timely manner as mentioned in Section 8.3,

iii. Without prejudice to the foregoing, in the event of a personal data breach, the person(s) responsible for such breach shall be liable in accordance with the provisions of applicable laws.

13.3 COMPLIANCE AND GUIDELINES GOVERNANCE

i. The DPO of the PDPO together with the DPO of the Ministry of Health shall ensure adherence to these Guidelines and shall be responsible for compliance with all Uganda applicable laws in force.

ii. All individuals and entities who are covered by these Guidelines must comply with its requirements and, where requested, demonstrate such compliance.

iii. The compliance checklists developed (Appendix I and III) shall be used for the purpose of monitoring the compliance of stakeholders to these guidelines.

iv. These Guidelines may be revised from time to time. A copy of these Guidelines together with any significant revisions shall be made publicly available through the Ministry of Health official communication channels like e-Library or the Knowledge Management Portal.

13.4 NON-COMPLIANCE WITH THESE GUIDELINES

Where any person to whom these Guidelines is applicable is found to be in violation of any of its provisions, such a person may not be permitted to participate in the national healthcare enterprise and further action shall be taken by the PDPO.

13.5 LIABILITY, PENALTIES AND REMEDIES

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

13.6 SALE OF HEALTH DATA

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

14.0 DISSEMINATION AND ADOPTION OF THE GUIDELINES

The Health Data Protection, Privacy and Confidentiality Guidelines shall be disseminated for adoption.

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

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

APPENDIX I: COMPLIANCE CHECKLIST FOR DATA CONTROLLERS TO ALIGN WITH THE GUIDELINES

1. Lawful basis and transparency

- Conduct an information audit to determine what information you process and who has access to it.
- Have a legal justification for your data processing activities.
- Provide clear information about your data processing and legal justification in your privacy guidelines.

2. Data security

- Take data protection into account at all times, from the moment you begin developing a product to each time you process data.
- Encrypt, pseudonymize or anonymize personal data wherever possible.
- Create internal security guidelines for your team members and build awareness about data protection.
- Know when to conduct a data protection impact assessment and have a process in place to carry it out.
- Have a process in place to notify the authorities and your data subjects in the event of a data breach.

3. Accountability and governance

- Designate someone responsible for ensuring guidelines compliance across your organization.
- Sign a data processing agreement between your organization and any third parties that process personal data on your behalf.
- Appoint a data protection officer (if necessary).

4. Privacy Rights

Ensure that it is easy for customers to:

- Request and receive all the information you have about them.
- Correct or update inaccurate or incomplete information.
- Request to have their personal data deleted.
- Ask you to stop processing their data.

- Receive a copy of their personal data in a format that can be easily transferred to another organisation.
- Object to you processing their data.
- Protect their rights if you make decisions about people based on automated processes.

APPENDIX II: PRIVACY NOTICE TEMPLATE

Sample: Department/Organization Privacy Notice

[Insert name of department/organization] is part of the [insert name of organization/ministry],]. This privacy notice shall explain how “[Insert name of department/organization] uses the personal data it collects from you when you use “[Insert name of department/organization] system.

1. **What data do** Insert name of department/organization] **collect?**

   “[Insert name of department/organization] collects the following data:

   - Personal identifiers (e.g., name, email address, phone number).
   - [Add any other data “[Insert name of department/organization] collects].

2. **How do** “[Insert name of department/organization] **collect your data?**

   You directly provide “[Insert name of department/organization] with most of the data Insert name of department/organization] collect. “[Insert name of department/organization] collect data and process data when you:

   - Register online or place an order for any of “[Insert name of department/organization] products or services.
   - Voluntarily complete a customer survey or provide feedback on any of “[Insert name of department/organization] message boards or via email.
   - Use or view “[Insert name of department/organization] website via your browser’s cookies.
   - [Add any other data “(Insert name of department/organization) collects].
   - Insert name of department/organization] may also receive your data indirectly from the following sources:
   - [Add any indirect source of data your Insert name of department/organization has].

3. **How will** Insert name of department/organization] **use your data?**

   Insert name of department/organization] collects your data so that it can:

   - Process your order and manage your account.
   - Email you with special offers on other products and services it thinks you might like.
   - [Add how else Insert name of department/organization] uses data].

   If you agree, Insert name of department/organization] will share your data with the following partner Department(s)/Organization(s) so that they may offer you their products and services:

- [List organizations that will receive data].

When Insert name of department/organization] processes your order, it may send your data to, and also use the resulting information from, National Digital Health Authority reference agencies to prevent fraudulent activities.

4. **How do** Insert name of department/organization] **store your data?**

Insert name of department/organization] securely stores your data at [insert the location and describe security precautions taken].

Insert name of department/organization] will keep your [insert type of data] for [insert time period]. Once this time period has expired, Insert name of department/organization] will delete your data by [insert how you delete user data].

5. **What are your data protection rights?**

Insert name of department/organization] would like to make sure you are fully aware of all of your data protection rights. Every user is entitled to the following:

- Confirmation and access: You have the right to request Insert name of department/organization] for copies of your personal data. Insert name of department/organization] may charge you a small fee for this service.
- Correction and erasure: You have the right to request that Insert name of department/organization] correct any information you believe is inaccurate. You also have the right to request Insert name of department/organization]to complete the information you believe is incomplete. You have the right to request that Insert name of department/organization] erase your personal data, under certain conditions.
- Restriction or objection to disclosure: You have the right to request that Insert name of department/organization] restricts the processing of your personal data, under certain conditions. You have the right to object to Insert name of department/organization] processing of your personal data, under certain conditions.
- Automated individual decision-making: You have the right to request Insert name of department/organization] not to subject you to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you unless you provide explicit consent by accepting our privacy notice.

If you make a request, Insert name of department/organization] have one month to respond to you. If you would like to exercise any of these rights, please contact us by any of the following means:

Email us at:

Call us at:

Or write to us at:

6. **What are cookies?**

   Cookies are text files placed on your computer to collect standard internet login information and visitor behavior information. When you visit Insert name of department/organization] website, Insert name of department/organization] may collect information from you automatically through cookies or similar technology. For further information, visit allaboutcookies.org.

7. **How do** Insert name of department/organization] **use cookies?**

   Insert name of department/organization] uses cookies in a range of ways to improve your experience on our website, including:

   - Keeping you signed in.
   - Understanding how you use [Insert name of department/organization] website to improve user experience.
   - [Add any uses your [Insert name of department/organization] has for cookies].

8. **What types of cookies do [**Insert name of department/organization] **use?**

   There are a number of different types of cookies; however, Insert name of department/organization] website uses:

   - Functionality cookies [Insert name of department/organization] uses these cookies so that Insert name of department/organization] recognize you on its website and remember your previously selected preferences. These could include what language you prefer and location you are in. A mix of first-party and third-party cookies are used. The first-party cookies are created by the domain while the third-party cookies are created by domains other than the [Insert name of department/organization] is visiting at the time, and are mainly used for tracking and online-advertising purposes
   - Advertising cookies – **[**Insert name of department/organization] uses these cookies to collect information about your visit to **[**Insert name of department/organization] website, the content you viewed, the links you followed, and information about your browser, device, and internet protocol address. The **[**Insert name of department/organization] sometimes shares some limited aspects of this data with third parties for advertising purposes. The **[**Insert name of department/organization] may also share data collected through cookies with **[**Insert name of department/organization] advertising partners. This means that when you visit another website, you may be shown advertising based on your browsing patterns on **[**Insert name of department/organization] website.

- [Add any other types of cookies your company uses].

9. How to manage cookies

You can set your browser not to accept cookies, and the website “allaboutcookies.org” tells you how to remove cookies from your browser. However, in a few cases, some of **[**Insert name of department/organization] website features may not function as a result.

10. Privacy policies of other websites

[Insert name of department/organization] website contains links to other websites. **[**Insert name of department/organization] privacy notice applies only to our website, so if you click on a link to another website, you should read their privacy notice.

11. Changes to our privacy policy

[Insert name of department/organization] keeps its privacy notice under regular review and places any updates on this web page. This privacy notice was last updated on [insert date in DD/MM/YYYY format].

12. How to contact us

If you have any questions about our **[**Insert name of department/organization]’s privacy notice, the data it holds on you, or you would like to exercise one of your data protection rights, please do not hesitate to contact **[**Insert name of department/organization]:

Email at:

Call at:

Or write to at:

13. How to contact the appropriate authority

Should you wish to report a complaint or if you feel that **[**Insert name of department/organization] has not addressed your concern in a satisfactory manner, you may contact the grievance redressal officer via:

Email:

Address:

APPENDIX III: DATA PROTECTION PRIVACY AND CONFIDENTIALITY CHECKLIST

Governance and Policy/Guidelines		Recommendations
Data Protection, Privacy and Confidentiality Policy/Guidelines	Does legislation or a guidance exist that covers the use of personally identifiable information (PII) for different purposes?	
Policy/Guidelines sections	Do the guidelines contain sections to ensure the privacy, confidentiality, and protection of PII? For example: ● Clearly defined roles and access levels for all persons with authorized access to PII. ● Clearly defined standard procedures or methods that must be followed when accessing PII. ● Information on the data life cycle (collection, storage, backup, use, transmission, release, disposal, etc.) ● Information on data breaches and breach investigations. ● Clearly defined training standards for organizations/entities.	
Policy/Guidelines distribution	Is the guidelines document distributed to stakeholders and relevant organizations? For example: ● Ministry to health staff at the national level. ● Health staff at regional/district/local facilities. ● Patients/data subjects at facilities. ● Academic researchers involved with PII data. ● Staff from donor organizations. ● Multilateral institution staff.	
Policy/Guidelines availability	Are the guidelines for ensuring confidentiality and security of PII readily accessible to all staff members? For example: ● Document available in multiple formats (hard copies, electronic).	

	● Document distributed to all staff members. ● Document easily accessible to all staff members at the facility.	
Policy/Guidelines development	Are stakeholders involved in the development of the guidelines document and its update process? For example: ● Health professionals (medical/nursing practitioners, public health specialists, other health professionals). ● Information technology specialists (data entry staff, analysts, managers, programmers). ● Patient advocacy groups. ● Legal experts. ● Human rights advocates and ethicists. ● Government officials. ● Business representatives. ● Support service staff (cleaners, security guards).	
Policy/Guidelines governance structure	Is there a governance structure such as an advisory committee in place to provide oversight for the appropriate collection, use, and dissemination of data, including regular review of the guidelines document and security practices?	
Covered uses of PII	Are there guidelines in the document on the uses of PII? For example: ● Individual health care ● Public health practice (including monitoring and evaluation) ● Human subjects research (with consent) ● Exceptional statutory purposes ● Other uses of PII	
Information security management	Are there guidelines within the document that require organizations to designate an information security manager? Is there a written description of the information security manager's responsibilities?	
Security breach management	Are there guidelines in the document for identifying and managing a security breach? For example:	

	● Definition of a security breach and its consequences ● Organizational structure and delineation of roles, responsibilities, and levels of authority ● Requirements for reporting security breaches ● Prioritization or severity ratings of security breaches ● Reporting and contact forms in the event of a breach	
Risk assessment	Are there guidelines in the document for risk assessments? If so, are these mandated assessments performed regularly?	
Review of security practices	Are security practices reviewed by independent auditors at regular intervals? Are information security and its management reviewed at regular intervals?	
Policy updating - advancements	Are there guidelines on how often software and hardware technologies are reviewed? Is the guidelines document regularly updated for advancements? For example: advancements in database software, web servers, email clients, firewalls, file servers, and backup devices	
Data Collection and Storage		
Interview privacy	Does your organization take measures for protecting patient privacy while collecting information (during the interview with the patient), such as: ● Minimizing the exchange of verbal information. ● Using a partition or curtain when using open rooms. ● Using a separate room with a soundproof barrier. ● Using cover sheets on paper documents. ● Using a computer screen guard that provides visual privacy?	
Inventory of paper-based	Is there an inventory of paper-based tools currently and previously used by the program?	

	Which paper-based tools should continue to be used as the level of disruption evolves?	
Protect paper-based data from unauthorized access	Are there measures in place to protect PII stored on paper from unauthorized access? For example: ● Locked cabinet ● Locked room ● Locked windows ● Bars/grills on doors or windows ● Alarm system ● Video monitoring ● Security guard or other authorized staff control access	
Protect paper-based tools from natural risks	Are there measures in place to protect PII stored on paper from natural risks? For example: ● Fire ● Water damage ● Animal damage (such as mice or termites)	
Inventory of database(s) with PII	Does your organization manage an updated inventory of database(s) and files containing PII, including their backups?	
Inventory electronic equipment with PII	Is there an inventory of electronic equipment (servers, desktop computers, laptop computer, tablets, smartphones, and other mobile devices) containing database(s)/files with PII?	
Protect electronic devices from natural risks	Are there measures in place to protect PII stored on electronic devices from natural risks? For example: ● Power failure (backup generator) ● Power surge (surge protector) ● Water damage (furniture and shelves to raise devices off floor) ● Fire (smoke detector, fire extinguisher) ● Extreme humidity (dehumidifier) ● Particulates—e.g., sand, ash, etc. (window and door screens, air purifier)	
Protect electronic devices from unauthorized access	Does your organization take measures for protecting PII stored on electronic devices from theft or destruction? For example:	

	● Locked cabinet ● Locked room ● Locked windows ● Bars/grills on doors or windows ● Alarm system ● Video monitoring ● Security guard or other authorized staff control access	
Antivirus	Does your organization take measures for protecting electronic devices against viruses? For example: ● Installing official antivirus software on all types of devices: servers, desktop computers, laptop computer, and other mobile devices such as smartphones ● Mechanism to update the antivirus signature in real time ● Mechanism to frequently perform full scan of the device ● Automated scan for all new files	
Firewall	Are there measures in place to protect networks against intrusion? For example: ● Adequate router configuration ● Installation of hardware or software firewall ● Anti-malware software ● Monitoring computers, servers, and network firewall logs	
Password policy	Is there a strong password policy in place? For example: ● All software/database(s) containing PII are password-protected. ● Passwords masked when entered into computer applications. ● There are constraints on the password (minimum length, combination of lowercase letters, uppercase letters, numbers, and special characters). ● Passwords must be changed frequently. ● Revocation of privilege as soon as employment is terminated. ● All files containing PII are password-protected.	

Anonymization	Are there measures in place to remove personal identifiers from data sets whenever possible (e.g., for analysis, statistics, external reporting)?	
Encryption	Are there procedures in place to ensure PII is always encrypted?	
Backup	Are there measures in place to securely back up data? For example: ● Adequate frequency for backups ● Backups on a distant, separate site ● Encryption of backups (especially with PII) ● Regular tests for restoral using backed-up data ● Secure storage of backed-up data media	
Multiple network connections	Are there guidelines in place for computers containing PII data that are connected to more than one network? For example: ● Use of built-in encryption on these devices ● Use of virtual private networks ● Remote desktop software ● Multiple network interface cards ● Network bridge	
Authorization and Access Control		
Data access by staff	Has staff member access to data been defined? For example, access by: ● Health professionals (medical practitioners, nursing practitioners, public health specialists, other health professionals) ● Access by information technology staff (data clerks, analysts, managers, programmers) ● Administrative staff ● Professional service providers ● Volunteers ● Academic or other researchers ● Support services (cleaners, security guards) ● Bilateral donor staff ● Multilateral institution staff	
Levels of access	For roles where access to data has been defined, are levels of access specified for using data for different purposes? For example:	

	● Individual health care use ● Public health practice use	
System security controls	Are there requirements in place to ensure system security controls are independently validated?	
Session timeout	Are there procedures in place to “timeout” or lock user sessions after a specified period of inactivity on software applications that contain PII?	
Data Transmission, Sharing, and Release		
Data release	Are there guidelines in place for data release? For example: ● Class of use for which data may be released. ● Specific data elements by which data may be released. ● Entities or organizations to whom data may be released. ● Requirements for how recipients will protect the confidentiality of received data. ● Specifications for time limitations on the use of released data. ● Data quality standards that must be met before data release. ● Clearly defined individual(s) who are authorized to release data. ● Clear procedures for handling data requests that not covered under the data release policy.	
Protect paper-based transmission	Are there procedures in place to protect paper-based documents with PII when they leave a site? For example: ● The amount and sensitivity of information contained in any piece of correspondence remains minimal. ● Documents are put in a sealed envelope. ● Mail marked “confidential” is only opened by the addressee. ● Documents are carried in a locked suitcase. ● Documents are carried only by authorized person(s).	

	● The person in charge of receiving the confidential mail must contact the sender to notify them that the mail was received.	
Protect electronic transmission	Are there procedures in place to protect data (password protection, encryption, acknowledgement of receipt) when information transits between systems/persons through: ● Email ● Intranet, a local-area network, wide-area network ● Internet (via web browser) ● File transfer protocol ● Tape, optical media ● Flash drive/memory stick/memory card ● External hard drive?	
Data release conditions	Are there conditions that must be met before releasing PII? For example: ● Verification that consent was obtained ● Confirmation that data was reviewed for accuracy ● Removal of direct patient identifiers from released records ● Request reviewed to verify the minimum amount of data needed to satisfy the purpose ● Acquisition of formal approval for data release	
Data release procedures - purpose	Are there procedures in place for data release (and/or data sharing) that control access to, and use of, individual-level information, covering the following cases: ● Individual health care (including sharing patient records with another facility when the patient is referred or transferred)? ● Sharing patient records with the patient directly (including sharing laboratory results with the patient via mail/email/SMS, etc.) ● Public health practice, including monitoring and evaluation or case reporting ● Human subjects research (with consent) ● Exceptional statutory purposes?	

Data release procedures - recipients	Are there procedures in place to protect PII when releasing it? For example: ● Asking the recipient to sign a confidentiality agreement. ● Asking the recipient for documentation of security training. ● Assessment of recipient organization security (review of procedural, electronic, and physical security controls). ● Recipient agreement to destroy information after data release purpose has been fulfilled. ● Internal steering group review and approval. ●	
Data anonymization	Are there procedures in place to explore alternatives to using identifiable data before sharing data, such as using anonymized or coded data?	
Data Disposition		
Data disposition procedures	Are there procedures in place to securely archive PII on paper-based tools when no longer in use?	
Disposition of paper-based information	Are there measures in place to securely dispose of PII stored on paper (e.g., forms, registers) and no longer used, such as: ● shredding documents containing PII with a cross-cutting shredder before disposing of them ● keeping records of documents destroyed?	
Data disposition procedures	Are there procedures in place to archive PII stored in electronic devices when no longer in use?	
Disposition of electronic-based information	Are there measures in place to securely dispose of PII stored electronically and no longer used, such as: ● eliminating emails sent or received containing PII ● sanitizing or destroying hard drives or mobile devices (including USB keys) that	

	contain PII before the computer/mobile device is reassigned to non-program staff members, sent off-site for repair, sold, or sent to garbage ● keeping records of documents destroyed ● asking partnering organizations to do the same?	
Data archival	Are there guidelines included on archiving data? For example: ● how often data must be archived ● approved storage locations of archived data ● approved media for archiving data ● roles responsible for archiving data	
Data migration	Are there procedures in place that require that data be periodically migrated to newer technologies as they become available?	
Data Disposal	Are there requirements for data retirement and record destruction? For example: ● data retirement schedule ● certification/verification of data disposal/destruction	

APPENDIX IV: ASSESSING AND IMPROVING CYBERSECURITY MATURITY

This appendix was adapted from the United States Department of Defense's Cybersecurity Maturity Model Certification, which measures cybersecurity maturity with up to three levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats. The model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references. Please note that 110 CMMC2 controls originate from NIST SP 800-171 r2.

Recommended practices for each of the maturity practice areas:

1. ACCESS CONTROL (AC)

Level 1

AC.L1-3.1.1 – **Authorized Access Control** – Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

AC.L1-3.1.2 – **Transaction & Function Control** – Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

AC.L1-3.1.20 – **External Connections** – Verify and control/limit connections to and use of external information systems.

AC.L1-3.1.22 – **Control Public Information** – Control information posted or processed on publicly accessible information systems.

Level 2

AC.L2-3.1.3 – **Control CUI Flow** – Control the flow of CUI in accordance with approved authorizations.

AC.L2-3.1.4 – **Separation of Duties** – Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

AC.L2-3.1.5 – **Least Privilege** – Employ the principle of least privilege, including for specific security functions and privileged accounts.

AC.L2-3.1.6 – **Non-Privileged Account Use** – Use non-privileged accounts or roles when accessing non-security functions.

AC.L2-3.1.7 – **Privileged Functions** – Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

AC.L2-3.1.8 – **Unsuccessful Logon Attempts** – Limit unsuccessful logon attempts.

AC.L2-3.1.9 – **Privacy & Security Notices** – Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules.

AC.L2-3.1.10 – **Session Lock** – Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

AC.L2-3.1.11 – **Session Termination** – Terminate (automatically) user sessions after a defined condition.

AC.L2-3.1.12 – **Control Remote Access** – Monitor and control remote access sessions.

AC.L2-3.1.13 – **Remote Access Confidentiality** – Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

AC.L2-3.1.14 – **Remote Access Routing** – Route remote access via managed access control points.

AC.L2-3.1.15 – **Privileged Remote Access** – Authorize remote execution of privileged commands and remote access to security-relevant information.

AC.L2-3.1.16 – **Wireless Access Authorization** – Authorize wireless access prior to allowing such connections.

AC.L2-3.1.17 – **Wireless Access Protection** – Protect wireless access using authentication and encryption.

AC.L2-3.1.18 – **Mobile Device Connection** – Control connection of mobile devices.

AC.L2-3.1.19 – **Encrypt CUI on Mobile** – Encrypt CUI on mobile devices and mobile computing platforms.

AC.L2-3.1.21 – **Portable Storage Use** – Limit use of portable storage devices on external systems.

2. AWARENESS AND TRAINING (AT)

Level 2

AT.L2-3.2.1 – **Role-Based Risk Awareness** – Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

AT.L2-3.2.2 – **Role-Based Training** – Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

AT.L2-3.2.3 – **Insider Threat Awareness** – Provide security awareness training on recognizing and reporting potential indicators of insider threat.

3. AUDIT AND ACCOUNTABILITY (AU)

Level 2

AU.L2-3.3.1 – **System Auditing** – Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

AU.L2-3.3.2 – **Event Review** – Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

AU.L2-3.3.3 – **Event Review** – Review and update logged events.

AU.L2-3.3.4 – **Audit Failure Alerting** – Alert in the event of an audit logging process failure.

AU.L2-3.3.5 – **login2Correlation** – Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

AU.L2-3.3.6 – **Reduction & Reporting** – Provide audit record reduction and report generation to support on-demand analysis and reporting.

AU.L2-3.3.7 – **Authoritative Time Source** – Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

AU.L2-3.3.8 – **Audit Protection** – Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

AU.L2-3.3.9 – **Audit Management** – Limit management of audit logging functionality to a subset of privileged users.

4. CONFIGURATION MANAGEMENT (CM)

Level 2

CM.L2-3.4.1 – **System Baselining** – Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

CM.L2-3.4.2 – **Security Configuration Enforcement** – Establish and enforce security configuration settings for information technology products employed in organizational systems.

CM.L2-3.4.3 – **System Change Management** – Track, review, approve, or disapprove, and log changes to organizational systems.

CM.L2-3.4.4 – **Security Impact Analysis** – Analyze the security impact of changes prior to implementation.

CM.L2-3.4.5 – **Access Restrictions for Change** – Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

CM.L2-3.4.6 – **Least Functionality** – Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

CM.L2-3.4.7 – **Nonessential Functionality** – Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

CM.L2-3.4.8 – **Application Execution Policy** – Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

CM.L2-3.4.9 – **User-Installed Software** – Control and monitor user-installed software.

5. IDENTIFICATION AND AUTHENTICATION (IA)

Level 1

IA.L1-3.5.1 – Identification

Identify information system users, processes acting on behalf of users, or devices.

IA.L1-3.5.2 – Authentication
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Level 2

IA.L2-3.5.3 – **Multi Factor Authentication** – Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

IA.L2-3.5.4 – **Replay-Resistant Authentication** – Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

IA.L2-3.5.5 – **Identifier Reuse** – Prevent the reuse of identifiers for a defined period.

IA.L2-3.5.6 – **Identifier Handling** – Disable identifiers after a defined period of inactivity.

IA.L2-3.5.7 – **Password Complexity** – Enforce a minimum password complexity and change of characters when new passwords are created.

IA.L2-3.5.8 – **Password Reuse** – Prohibit password reuse for a specified number of generations.

IA.L2-3.5.9 – **Temporary Passwords** – Allow temporary password use for system logins with an immediate change to a permanent password.

IA.L2-3.5.10 – **Cryptographically-Protected Passwords** – Store and transmit only cryptographically protected passwords.

IA.L2-3.5.11 – **Obscure Feedback** – Obscure feedback of authentication information.

6. INCIDENT RESPONSE (IR)

Level 2

IR.L2-3.6.1 – **Incident Handling** – Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user-response activities.

IIR.L2-3.6.2 – **Incident Reporting** – Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

IR.L2-3.6.3 – **Incident Response Testing** – Test the organizational incident response capability.

7. MAINTENANCE (MA)

Level 2

MA.L2-3.7.1 – **Perform Maintenance** – Perform maintenance on organizational systems.

MA.L2-3.7.2 – **System Maintenance Control** – Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

MA.L2-3.7.3 – **Equipment Sanitization** – Ensure equipment removed for off-site maintenance is sanitized of any CUI.

MA.L2-3.7.4 – **Media Inspection** – Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

MA.L2-3.7.5 – **Nonlocal Maintenance** – Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

MA.L2-3.7.6 – **Maintenance Personnel** – Supervise the maintenance activities of personnel without required access authorization.

8. MEDIA PROTECTION (MP)

Level 1

MP.L1-3.8.3 – **Media Disposal** – Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

Level 2

MP.L2-3.8.1 – **Media Protection** – Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

MP.L2-3.8.2 – **Media Access** – Limit access to CUI on system media to authorized users.

MP.L2-3.8.4 – **Media Markings** – Mark media with necessary CUI markings and distribution limitations.

MP.L2-3.8.5 – **Media Accountability** – Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

MP.L2-3.8.6 – **Portable Storage Encryption** – Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

MP.L2-3.8.7 – **Removable Media** – Control the use of removable media on system components.

MP.L2-3.8.8 – **Shared Media** – Prohibit the use of portable storage devices when such devices have no identifiable owner.

MP.L2-3.8.9 – **Protect Backups** – Protect the confidentiality of backup CUI at storage locations.

9. PERSONNEL SECURITY (PS)

Level 2

PS.L2-3.9.1 – **Screen Individuals** – Screen individuals prior to authorizing access to organizational systems containing CUI.

PS.L2-3.9.2 – **Personnel Actions** – Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

10. PHYSICAL PROTECTION (PE)

Level 1

PE.L1-3.10.1 – **Limit Physical Access** – Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

PE.L1-3.10.3 – **Escort Visitors** – Escort visitors and monitor visitor activity.

PE.L1-3.10.4 – **Physical Access Logs** – Maintain audit logs of physical access.

PE.L1-3.10.5 – **Manage Physical Access** – Control and manage physical access devices.

Level 2

PE.L2-3.10.2 – **Monitor Facility** – Protect and monitor the physical facility and support infrastructure for organizational systems.

PE.L2-3.10.6 – **Alternative Work Sites** – Enforce safeguarding measures for CUI at alternate work sites.

11. RISK ASSESSMENT (RA)

Level 2

RA.L2-3.11.1 – **Risk Assessments** – Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

RA.L2-3.11.2 – **Vulnerability Scan** – Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

RA.L2-3.11.3 – **Vulnerability Remediation** – Remediate vulnerabilities in accordance with risk assessments.

12. SECURITY ASSESSMENT (CA)

Level 2

CA.L2-3.12.1 – **Security Control Assessment** – Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

CA.L2-3.12.2 – **Plan of Action** – Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

CA.L2-3.12.3 – **Security Control Monitoring** – Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

CA.L2-3.12.4 – **System Security Plan** – Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

13. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Level 1

SC.L1-3.13.1 – **Boundary Protection** – Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

SC.L1-3.13.5 – **Public-Access System Separation** – Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Level 2

SC.L2-3.13.2 – **Security Engineering** – Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

SC.L2-3.13.3 – **Role Separation** – Separate user functionality from system management functionality.

SC.L2-3.13.4 – **Shared Resource Control** – Prevent unauthorized and unintended information transfer via shared system resources.

SC.L2-3.13.6 – **Network Communication by Exception** – Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

SSC.L2-3.13.7 – **Split Tunneling** – Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

SC.L2-3.13.8 – **Data in Transit** – Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

SC.L2-3.13.9 – **Connections Termination** – Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

SC.L2-3.13.10 – **Key Management** – Establish and manage cryptographic keys for cryptography employed in organizational systems.

SC.L2-3.13.11 – **CUI Encryption** – Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

SC.L2-3.13.12 – **Collaborative Device Control** – Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

SC.L2-3.13.13 – **Mobile Code** – Control and monitor the use of mobile code.

SC.L2-3.13.14 – **Voice over Internet Protocol** – Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

SC.L2-3.13.15 – **Communications Authenticity** – Protect the authenticity of communications sessions.

SC.L2-3.13.16 – **Data at Rest** – Protect the confidentiality of CUI at rest.

14. SYSTEM AND INFORMATION INTEGRITY (SI)

Level 1

SI.L1-3.14.1 – **Flaw Remediation** – Identify, report, and correct information and information system flaws in a timely manner.

SI.L1-3.14.2 – **Malicious Code Protection** – Provide protection from malicious code at appropriate locations within organizational information systems.

SI.L1-3.14.4 – **Update Malicious Code Protection** – Update malicious code protection mechanisms when new releases are available.

SI.L1-3.14.5 – **System & File Scanning** – Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Level 2

SI.L2-3.14.3 – **Security Alerts & Advisories** – Monitor system security alerts and advisories and take action in response.

SI.L2-3.14.6 – **Monitor Communications for Attacks** – Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

SI.L2-3.14.7 – Identify Unauthorized Use – Identify unauthorized use of organizational systems.

APPENDIX V: DATA PROCESSING AGREEMENT TEMPLATE

[This appendix contains a sample data processing agreement between a data processor and a department/unit of the Ministry of Health. It includes guidelines that the data processor shall follow to maintain data protection, privacy and confidentiality and to ensure the rights of data subjects.]

This Data Processing Agreement ("Agreement") forms part of the Contract for

Services ("Principal Agreement") between

____

____

____

(the “[Department/Unit of the Ministry of Health]”)

And

____

____

____

(the “Data Processor”)

(together as the “Parties”)

WHEREAS

(A) The [Department/Unit of the Ministry of Health] acts as a Data Controller.

(B) The [Department/Unit of the Ministry of Health] wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a Data Processing Agreement that complies with the requirements of the current legal framework in relation to data processing and with Data Protection and Privacy Act 2019 regarding the processing of personal data and on the free movement of such data.

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "[Department/Unit of the Ministry of Health] Personal Data" means any personal data processed by a Contracted Processor on behalf of [Department/Unit of the Ministry of Health] pursuant to or in connection with the Principal Agreement;

1.1.3 "Contracted Processor" means a Subprocessor;

1.1.4 "Data Protection Laws" means Data Protection and Privacy Act 2019 and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.8 "Data Transfer" means:

1.1.8.1 a transfer of [Department/Unit of the Ministry of Health] Personal Data from the [Department/Unit of the Ministry of Health] to a Contracted Processor; or

1.1.8.2 an onward transfer of [Department/Unit of the Ministry of Health] Personal Data from a Contracted Data Processor to a Subcontracted Data Processor, or between two establishments of a Contracted Processor,

In each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "Services" means the [__________________] services the [Department/Unit of the Ministry of Health] provides.

1.1.10 "Subprocessor" means any person appointed by or on behalf of the Data Processor to receive and process Personal Data on behalf of the [Department/Unit of the Ministry of Health] in connection with the Agreement.

2. Processing of [Department/Unit of the Ministry of Health] Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of [Department/Unit of the Ministry of Health] Personal Data; and

2.1.2 not process [Department/Unit of the Ministry of Health] Personal Data other than on the relevant [Department/Unit of the Ministry of Health] documented instructions;

2.2 The [Department/Unit of the Ministry of Health] instructs Data Processor to process [Department/Unit of the Ministry of Health] Personal Data.

3. Processor Personnel

Data Processor shall take reasonable steps to ensure the reliability of any employee, agent, or contractor of any Contracted Processor who may have access to the [Department/Unit of the Ministry of Health] Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant [Department/Unit of the Ministry of Health] Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processor shall in relation to the [Department/Unit of the Ministry of Health] Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in [Relevant Country Policy/Guidelines].

4.2 In assessing the appropriate level of security, Data Processor shall take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 Data Processor shall not appoint (or disclose any [Department/Unit of the Ministry of Health] Personal Data to) any Subprocessor unless required or authorized by the [Department/Unit of the Ministry of Health].

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Data Processor shall assist the [Department/Unit of the Ministry of Health] by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the [Department/Unit of the Ministry of Health] obligations, as reasonably understood by [Department/Unit of the Ministry of Health], to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Data Processor shall:

6.2.1 promptly notify [Department/Unit of the Ministry of Health] if it receives a request from a Data Subject under any Data Protection Law in respect of [Department/Unit of the Ministry of Health] Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of [Department/Unit of the Ministry of Health] or as required by applicable laws to which the Data Processor is subject, in which case Data Processor shall to the extent permitted by applicable laws inform [Department/Unit of the Ministry of Health] of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Data Processor shall notify [Department/Unit of the Ministry of Health] without undue delay upon Data Processor becoming aware of a Personal Data Breach affecting [Department/Unit of the Ministry of Health] Personal Data, providing [Department/Unit of the Ministry of Health] with sufficient information to allow the [Department/Unit of the Ministry of Health] to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Data Processor shall cooperate with the [Department/Unit of the Ministry of Health] and take reasonable commercial steps as are directed by [Department/Unit of the Ministry of Health] to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Data Processor shall provide reasonable assistance to the [Department/Unit of the Ministry of Health] with any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, which [Department/Unit of the Ministry of Health] reasonably considers to be required by Data Protection and Privacy Act 2019 or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of [Department/Unit of the Ministry of Health] Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or Return of [Department/Unit of the Ministry of Health] Personal Data

9.1 Subject to this paragraph, Data Processor shall promptly and in any event within ten (10) business days of the date of cessation of any Services involving the Processing of [Department/Unit of the Ministry of Health] Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those [Department/Unit of the Ministry of Health] Personal Data.

9.2 Data Processor shall provide written certification to [Department/Unit of the Ministry of Health] that it has fully complied with this paragraph (9.1-.9.2) within ten (10) business days of the Cessation Date.

10. Audit Rights

10.1 Subject to this paragraph, Data Processor shall make available to the [Department/Unit of the Ministry of Health] on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the [Department/Unit of the Ministry of Health] or an auditor mandated by the [Department/Unit of the Ministry of Health] in relation to the Processing of the [Department/Unit of the Ministry of Health] Personal Data by the Contracted Processors.

10.2 Information and audit rights of the [Department/Unit of the Ministry of Health] only arise under paragraph 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Data Processor may not transfer or authorize the transfer of Personal Data to other countries without the prior written consent of the [Department/Unit of the Ministry of Health]. If Personal Data processed under this Agreement are transferred to or from another country, the Parties shall ensure that the Personal Data are adequately protected.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and shall be delivered personally, sent by post to the mailing address, or sent by email to the email address set out in the heading of this Agreement or at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of [________________.]

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of [_________________], subject to possible appeal to [___________________________________].

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

[Department/Unit of the Ministry of Health]

Signature _______________________________

Name: _________________________________

Title: ________________________________

Date Signed: __________________________

Data Processor

Signature _____________________________

Name ________________________________

Title _________________________________

Date Signed __________________________