LAGOS UNIVERSITY TEACHING HOSPITAL
DATA PROTECTION POLICY AND PROCEDURES

Policy Statement:
Lagos University Teaching Hospital (herein and after referred to as "LUTH") obtains, uses, stores, and otherwise processes personal data relating to data subjects which includes patients of LUTH. When processing personal data, LUTH is obliged to complying with provisions of the Nigeria Data Protection Act (NDPA), Nigeria Data Protection Regulations (NDPR) and other relevant data protection laws, regulations and principles in Nigeria.

LUTH has in place policies, procedures, controls, and measures to ensure compliance with these data protection laws, regulations and principles. Ensuring and maintaining the security and confidentiality of personal information of data subjects is a priority consideration of the hospital.

Purpose:
The purpose of this policy is to ensure that LUTH meets its legal, statutory and regulatory requirements under the data protection laws regulations and principles in Nigeria, and to ensure that all personal data is processed in compliances with the extant data protection laws, regulations and principles.

This policy ensures that LUTH is clear about how personal data is and must be processed as well as LUTH's expectations for all those who process personal data on its behalf; in order to comply with the data protection laws, regulations and principles in Nigeria. The policy also ensures that personal data entrusted to LUTH is processed in accordance with data subjects' rights and protects LUTH from risks of personal data breaches and other breaches of data protection laws, regulations and principles in Nigeria.

In addition, this policy serves as guidance for employees and third-party agents on the responsibilities of handling and accessing personal data and data subject requests.

Scope:
This policy applies to all personal data processed by LUTH regardless of the data subject, what form the personal data is collected and in what format it is stored. All staff of LUTH as well as third party agents processing personal data on behalf of LUTH must adhere to this policy and non-compliance may lead to disciplinary action.

This policy is displayed publicly on LUTH's website and social media handles.

Personal Data Protection Principles:
LUTH is guided by the NDPA, NDPR and other relevant data protection laws, regulations and principles in Nigeria. These laws, regulations and principles require that:

1. Personal data shall be:
    a) Collected and processed in accordance with specific, legitimate and lawful purpose consented to by the data subject; provided that:

i. Any further processing may be done only for archiving, scientific research, historical research or statistical purposes for public interest.
ii. Any person or entity carrying out or purporting to carry out data processing under the provision of this paragraph shall not transfer any personal data to any person.

b) Adequate, accurate and without prejudice to the dignity of human person;
c) Stored only for the period within which it is reasonably needed, and
d) Secured against all foreseeable hazards and breaches such as theft, cyberattack, virus attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements.

2. Anyone who is entrusted with personal data of a data subject or who is in possession of the Personal Data of a Data Subject owes a duty of care to the said Data Subject;
3. Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject shall be accountable for his acts and omissions in respect of data processing, and in accordance with the principles contained in this Regulation.

Basis for Processing of Personal Data:

Processing of personal data by a public institution, including LUTH must be founded on Public, Legal and Vital interest and the determination of these bases shall be subject to the following:

1. The processing is directly or collaterally linked to the performance of a mandate stipulated by an Act of the National Assembly.
2. The processing is necessary for the promotion of the security or welfare of the citizens, justifiable in a democratic and free society.
3. A directive of the President in furtherance of the powers vested on that office by the Constitution or a legal instrument.

Processing of personal data shall be lawful and legitimate on any of the following basis:

1. Clear consent of the data subject for one or more specific purposes;
2. Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. Compliance with a legal obligation to which the institution is subject;
4. Protection of the vital interests of the data subject or of another natural person;
5. Processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the controller;
6. Legitimate interest of the data subject;

Requirement of Consent:

Under the NDPR, consent shall be required for the purpose of processing personal data in the following circumstances, even where another legal basis for processing also applies:

1. For the processing of sensitive personal data such as health, ethnic, political affiliation, religious beliefs, trade union membership, biometric, genetic and sexual orientation.

2. Where personal data is used for purposes other than those initially specified to the data subject.
3. Where personal data relating to a child is processed, in which case, consent is given by the parent or guardian.
4. Before personal data is processed outside Nigeria.
5. Before the data controller makes a decision based solely on automated processing which produces legal effects concerning or significantly affecting the data subject.
6. For any direct marketing or communication activity, except to existing data subjects who have accessed a service and given consent earlier.

Responsibilities of LUTH:

As a Data Controller, LUTH has the responsibility of putting in place policies and procedures that comply with the NDPA, NDPR and other relevant data protection laws, regulations and principles in Nigeria.

These policies and procedures ensure that:

1. LUTH protects the rights of individuals with regards to the processing of personal information.
2. LUTH develops, implements, and maintains a data protection policy, procedure, audit plan and training program for compliance with the data protection laws.
3. Every function and process carried out by LUTH, is monitored for compliance with extant data protection laws, regulations and principles in Nigeria.
4. Personal data is only processed after verification of the appropriateness and legal basis of the processing requirements.
5. LUTH obtains consent from data subject prior to collection of personal data and that all such consent are recorded and stored appropriately.
6. All employees of LUTH and third-party agents are aware of their data protection obligations and responsibilities as contained in the NDPA, NDPR and other relevant data protection laws, regulations and principles in Nigeria.
7. These obligations and responsibilities are reinforced through regular in-house training on the data protection laws, principles, regulations and how they apply to their specific roles.
8. LUTH maintains a continuous program of monitoring, review, and improvement regarding compliance with extant data protection laws, regulations and principles in Nigeria and to identify gaps and non-compliance before they become a risk, effecting mitigating actions where necessary.

Under the NDPA, NDPR and other relevant data protection laws, regulations and principles in Nigeria, the following are the responsibilities of LUTH:

1. To take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and for any information relating to a child. The information shall be

provided in writing, or by other means, including, where appropriate, by electronic means.

2. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
3. If LUTH does not act on the request of the data subject, the hospital shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority.
4. Except as otherwise provided by any public policy or Regulation, information provided to the data subject and any communication and any actions taken shall be provided free of charge.
5. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, LUTH may either:
    a. Charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested; or,
    b. Write a letter to the Data Subject stating refusal act on the request and copy National Information Technology Development Agency (NITDA).
6. LUTH shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
7. Where LUTH has reasonable doubts concerning the identity of the natural person making the request for information, LUTH may request the provision of additional information necessary to confirm the identity of the Data Subject.
8. The information to be provided to Data Subject may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing.
9. Where the icons are presented electronically, they shall be machine-readable.
10. LUTH shall developed and documented appropriate technical and organizational measures and controls for personal data security.
11. LUTH shall appoint a Data Protection Officer who shall be responsible for the overall supervision, implementation and ongoing compliance with the data protection laws and perform other specific duties as set out under NDPR.
12. LUTH shall have in place dedicated audit and monitoring programs to carry out regular checks and assessments on how the personal data processed is obtained, used, stored and shared.
13. LUTH shall provide clear reporting lines and supervision with regards to data protection.

Rights of Data Subjects:

Patients accessing care at LUTH and other data subjects have the following rights:

1. Prior to collecting Personal Data from a Data Subject, LUTH shall provide the Data Subject with all the following information:
    a. The identity and the contact details of LUTH;

b. The contact details of the Data Protection Officer;
c. The purpose(s) of the processing for which the Personal Data are intended as well as the legal basis for the processing;
d. Where applicable, the fact that the Controller intends to transfer Personal Data to a third country or international organization and the existence or absence of an adequacy decision by NITDA;
e. The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
f. The existence of the right to request from LUTH access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to Data Portability;
g. The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
h. The right to lodge a complaint with a relevant authority;
i. Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
j. The existence of automated decision-making, including profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the
k. Where the Controller intends to further process the Personal Data for a purpose other than that for which the Personal Data were collected, the controller shall provide the Data Subject prior to that further processing with information on that other purpose, and with any relevant further information; and
l. Where applicable, that the Controller intends to transfer Personal Data to a recipient in a foreign country or international organization and the existence or absence of an adequacy decision by NITDA.

2. Where Personal Data are transferred to a foreign country or to an international organization, LUTH shall inform the Data Subject of the appropriate safeguards for data protection in the foreign country.
3. The Data Subject shall have the right to obtain from LUTH without undue delay the rectification of inaccurate Personal Data concerning him or her. Considering the purposes of the processing, the Data Subject shall have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.
4. The Data Subject shall have the right to request LUTH to delete Personal Data without delay, and LUTH shall delete Personal Data where one of the following grounds applies:
    a. the Personal Data are no longer necessary in relation to the purposes for which they were collected or processed;
    b. the Data Subject withdraws consent on which the processing is based;

c. the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;
d. the Personal Data have been unlawfully processed; and
e. the Personal Data must be erased for compliance with a legal obligation in Nigeria.

5. The Data Subject shall have the right to obtain from LUTH restriction of processing where one of the following applies:
    a. The accuracy of the Personal Data is contested by the Data Subject for a period enabling LUTH to verify the accuracy of the Personal Data;
    b. The processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
    c. LUTH no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defense of legal claims; and
    d. The Data Subject has objected to processing, pending the verification whether the legitimate grounds of LUTH override those of the Data Subject.
6. Where processing has been restricted such Personal Data shall, except for storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest in Nigeria.
7. LUTH communicate any rectification or erasure of Personal Data or restriction to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. LUTH shall inform the Data Subject about those recipients if the Data Subject requests it.
8. The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance from the controller to which the Personal Data have been provided, where:
    a. The processing is based on consent, or
    b. On a contract, and
    c. The processing is carried out by automated means.
9. In exercising his right to Data Portability, the Data Subject shall have the right to have the Personal Data transmitted directly from one controller to another, where technically feasible. Provided that this right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.
10. The exercise of the foregoing rights shall be in conformity with constitutionally guaranteed principles of law for the general protection and enforcement of fundamental rights.

Data Security:

LUTH has in place security measures to protect data; such measures include but are not limited:

1. Protecting systems from hackers.
2. Setting up firewalls.
3. Storing data securely with access restricted to specific authorized individuals.
4. Employing data encryption technologies.
5. Developing organizational policy for handling personal data (and other sensitive or confidential data).
6. Protection of emailing systems.
7. Continuous capacity building for staff.

Designation of a Data Protection Officer (DPO):

LUTH has designated a DPO who's duties and responsibilities in the hospital include the following:

1. Getting the Board and Management of LUTH to buy-in into data protection implementation.
2. Developing and constantly reviewing business case for data protection implementation.
3. Inculcating data protection as a culture.
4. Understanding the data processing activities of each operational unit.
5. Constant training and capacity development for staff, licensees, contractors and stakeholders on data protection and management.
6. Advising the Management on practices that could trigger breaches
7. Interpreting the roles of different units in the light of data privacy protection.

Responsibilities of LUTH Staff Processing Personal Data:

1. Staff members who process personal data about data subjects must comply with the
2. requirements of this policy.
3. Staff members must ensure that:
    a. All personal data is kept securely;
    b. No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party.
    c. Personal data is kept in accordance with LUTH policies and procedures
    d. Any queries regarding data protection, are promptly directed to the DPO.
    e. Any data protection breaches are immediately brought to the attention of the DPO, and that they support the DPO in resolving breaches.
    f. Where there is uncertainty around a data protection matter advice is sought from the DPO.

Data Breach:

A data breach is considered to have occurred whenever personal data is accessed, viewed, or shared by an unauthorized party without permission. The following events constitute a data breach:

1. Inappropriate access controls allowing unauthorized use.
2. Accidental sharing of data with someone who does not have a right to know this information, whether this is as a result of:
    a. Human error.
    b. Technology/equipment failure
3. A hacking attack.
4. Loss or theft of data or equipment on which data is stored.
5. Improper transmission of Personal Data across borders.

Data Breach Management:
A data breach procedure is established and maintained in order to deal with incidents concerning Personal Data or privacy practices leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

All employees must inform the DPO immediately whenever there is a violation of this policy or a suspected data breach. This ensures that:

1. In the case of violations of the policy, appropriate measures are taken to correct and prevent future recurrence of the breach.
2. In the cases of data breach:
    a. Immediate remedial actions, in respect of the breach, are taken.
    b. Affected data subjects are informed.
    c. Reporting obligations to NITDA or other regulatory authority are complied with.
    d. Other required stakeholder communications are addressed.

Upon receipt of a report of a data breach event, the DPO shall:
1. Validate the breach by reviewing all necessary documents.
2. If the breach is confirmed:
    a. Notify Hospital Management
    b. Ensure that impacted data subjects are appropriately notified.
    c. Ensure that a detailed investigation is initiated, conducted, documented, and concluded.
    d. Report findings of the investigation to the Hospital Management.
    e. Identify remediation requirements and track their resolution.
    f. Coordinate with appropriate authorities as needed.
    g. Coordinate internal and external communications.

Changes to this Policy
LUTH reserves the right to change, amend or alter this Policy at any point in time. Whenever policy is amended, an updated version shall be made public.