THE DUCHESS INTERNATIONAL HOSPITAL Data Privacy & Protection Policy

Table of Contents

1. INTRODUCTION

The DUCHESS international Hospital ("DUCHESS"), comprises of firms that offer wealth creation opportunities through a unique blend of traditional asset management, life insurance and alternative investment services including equities, fixed income securities, and real estate. It needs to gather and process certain information about individuals, both locally and internationally, with whom it has relationship for various purposes such as,

but not limited to relationship management with investors, customers, clients, recruitment and payment of staff etc.

In lieu of the emerging data protection regulatory framework which requires higher transparency and accountability on how companies manage and use personal data, DUCHESS must ensure that its business operations align with global best practices on protection of rights and privacy of individuals.

2. DATA PROTECTION REGULATIONS

The Nigeria Data Protection Regulation ("NDPR" or "the Regulation"), which came into force on January 25, 2019, regulates the gathering, storing and processing of personal data (regardless of whether data is stored electronically, on paper or on other materials), and protects the rights and privacy of all living individuals (including children). The Regulation applies to natural persons residing in Nigeria or residing outside Nigeria but of Nigeria descent

3. DEFINITIONS

a. Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
b. Data means characters, symbols and binary on which operations are performed by a computer which may be stored or transmitted in the form of electronic signals is stored in any format or any device.
c. Database means a collection of data organized in a manner that allows access, retrieval, deletion and procession of that data; it includes but not limited to structured, unstructured, cached and file system type databases.
d. Data Administrator means any person or organization that processes data.
e. Data Controller means a person who either alone, jointly with other persons or in common with other persons or as a statutory body, determines the purposes for and the way personal data is processed or is to be processed.
f. Data Portability means the ability for data to be transferred easily from one IT system or computer to another through a safe and secure means in a standard format.
g. NITDA means the Nigeria Information Technology Development Agency.
h. Data Protection Compliance Organization (DPCO) means any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with this Regulation or any foreign Data Protection law or regulation having effect in Nigeria.
i. Data Subject means an identifiable person; one who can be identified directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
j. Party means directors, shareholders, servants and privies of a contracting party.
k. Personal Data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others.

l. Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

m. Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

n. Record means public record and reports in credible news media.

o. Sensitive Personal Data means data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.

p. Relevant Regulatory Authorities shall include NITDA, Attorney General of the Federation or any other agent of the Government empowered to issue directives under the Regulation.

4. DATA PRIVACY NOTICE

The purpose of this policy is to:

a. Protect DUCHESS from the risks of a data breach;
b. Disclose how DUCHESS stores and processes individuals' data;
c. Protect the rights of staff, members and stakeholders; and
d. Comply with the Regulation and follow international best practices.

5. SCOPE OF POLICY

This Policy applies to all staff, Management and Board of DUCHESS, as well as those of its subsidiary entities and associated companies. As a matter of best practice, other companies (contractors, suppliers etc.), individuals working with DUCHESS and its stakeholders who have access to personal information. It is also applicable to all data that DUCHESS holds relating to identifiable individuals, even if that information technically falls outside of the Regulation. This includes, but not limited to: a. Names of individuals;

b. Email addresses;
c. Contact phone numbers; and
d. Any other information relating to the individuals.

6. POLICY GOVERNANCE

DUCHESS will be the data controller under the terms of the Regulation – this means it is ultimately responsible for controlling the use and processing of personal data. DUCHESS shall appoint a Data Protection Officer (DPO) for the purpose of ensuring adherence to this Regulation, relevant data privacy statements and data protection directives.

The Board and all those in managerial or supervisory roles throughout DUCHESS are responsible for developing and encouraging good information handling practices within DUCHESS; responsibilities are set out in individual job descriptions.

Data Protection Officer (DPO), shall be an employee with requisite skills and experience, and such individual shall be accountable to Executive Management within DUCHESS. He/she shall be responsible for managing personal data and for the purpose of ensuring adherence to this Regulation, relevant data privacy statements and data protection directives of DUCHESS.

The ownership and maintenance of this policy is the responsibility of the Data Protection Officer. The day-to-day responsibility of interpreting and communicating this policy provision to DUCHESS employees is also the responsibility of the Data Protection Officer.

7. General Policy Statement

DUCHESS is committed to compliance with all relevant Nigerian laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information DUCHESS collects and processes in accordance with the Nigeria Data Protection Regulation (NDPR).

The Regulation and this policy apply to all of DUCHESS personal data processing functions, including those performed on customers', clients, investors', employees', suppliers' and partners' personal data, and any other personal data the organization processes from any source.

Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to DUCHESS' activities and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's (NITDA) request.

This policy also applies to all employees or staff and third parties of DUCHESS, and shall be supported by DUCHESS' Code of Business Conduct & Ethics. Any breach of the NDPR will be dealt with under DUCHESS' Disciplinary Process & Sanctions Policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for DUCHESS, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by DUCHESS without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which DUCHESS is committed, and which gives DUCHESS the right to audit compliance with the agreement.

8. Governing Principles of Data Protection

The Regulation mandates every data controller to process any personal data in accordance with the governing principles of data protection. In order to comply with the obligations, DUCHESS undertakes to adhere to the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data.

8.1 Data Processing

The following statement shall guide compliance with the Regulation on data processing. DUCHESS shall:

a) Collect and process personal data in accordance with specific, legitimate and lawful purpose consented to by the data subject;

b) Take reasonable steps to ensure that any personal data is accurate;

c) Store personal data about an individual that is sufficient for the purpose it is holding it for in relation to that individual;

d) Store individuals' personal data only for the period within which it is reasonably needed;

e) Secure personal data against all foreseeable hazards, breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements;

f) Exercise duty of care of personal data in its possession; and

g) Be accountable for its acts and omissions in respect of data processing and in accordance with the Regulation.

8.2 Lawful Processing

DUCHESS shall process personal data of individuals if at least one of the following applies:

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) Processing is necessary for the performance of a contract to which data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) Processing is necessary for compliance with a legal obligation to which DUCHESS is subject;
d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person; and
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in DUCHESS.

8.3 Procuring Consent

To fulfil the requirement of the Regulation, personal data will be processed in accordance with the rights of data subject. DUCHESS business operations will be guided by the following statements:

a) DUCHESS shall not obtain personal data except the specific purpose of collection is made to the data subject;
b) DUCHESS shall ensure that consent of data subject has been obtained without fraud, coercion or undue influence;
c) DUCHESS shall ensure that the data subject has consented to processing of his or her personal data and the legal capacity to give consent, where processing is based on consent;
d) DUCHESS shall request for consent in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language, where the data subject's consent is given in the context of a written declaration;

e) DUCHESS shall inform the data subject his/her right and the ease to withdraw his/her consent at any time;
f) When DUCHESS is assessing whether consent is freely given, it shall take utmost account of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary or excessive for the performance of the contract; and
g) DUCHESS shall request for consent of the data subject where data may be transferred to a third party for any reason.

8.4 Due Diligence and Prohibition of Improper Motives

To align with these requirements, DUCHESS shall:

a) Not seek consent that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts; and
b) Take reasonable measures to ensure that a party to any data processing contract does not have a record of violating the Regulation and such party is accountable to NITDA or a reputable regulatory authority for data protection within or outside Nigeria.

8.5 Privacy Policy

DUCHESS shall display a simple and conspicuous privacy policy that the class of data subjects being targeted can understand, irrespective of the medium through which such personal data are being collected or processed. DUCHESS privacy policy shall contain the following:

a) Constitution of data subjects' consent;
b) Description of collectable personal information;
c) Purpose of collection of personal data;
d) Technical methods used to collect and store personal information, cookies, web tokens, etc.;
e) Access, if any, of third parties to personal data and purpose of access;
f) A highlight of the principles governing data processing;
g) Available remedies in the event of violation of the privacy policy;
h) The timeframe for remedy; and
i) Any limitation clause, provided that the limitation clause does not exonerate DUCHESS from breaches of the Regulation.

8.6 Data Security

DUCHESS recognizes the importance of protecting data from unauthorized access and data corruption and shall:

a) Develop security measures including but not limited to protecting systems from hackers;
b) Set up firewalls and protect email systems;
c) Store data securely with access to specific authorized individuals;
d) Employ data encryption technologies;
e) Develop organizational policy for handling personal data and other sensitive or confidential data; and
f) Continuously build capacity for all staff.

8.7 Third Party Data Processing Contracts

To ensure compliance with the Regulation, being a data controller, the DUCHESS shall:

a) Ensure that a written contract is signed by a third party that will process personal data of individuals; and
b) Ensure that such third party that will process the data obtained from data subjects complies with the Regulation.

8.8 Objections by the Data Subject

DUCHESS acknowledges that individuals have the right to object to the processing of their data, as such it shall only process personal data in accordance with data subjects' rights as listed below:

a) Option to object the processing of personal data relating to the data subject which DUCHESS intends to process for the purposes of marketing; and
b) Option to be expressly and manifestly offered the mechanism for objection to any form of data processing free of charge.

8.9 Transfer to a Foreign Country

DUCHESS shall comply with the Regulation and any transfer of personal data which is undergoing processing or is intended for processing after transfer to a foreign country or an international organization shall take place subject to the provisions of the Regulation.

8.10 Exceptions in Respect of Transfer to a Foreign Country

In the absence of any decision made by relevant regulatory authorities on the transfer of personal data to a foreign country, DUCHESS shall initiate the transfer or set of transfers of personal data to such foreign country or an international organization only when:

a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards and that there are no alternatives;
b) The transfer is necessary for the performance of a contract between the data subject and DUCHESS or the implementation of pre-contractual measures taken at the data subject's request;
c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between DUCHESS and another natural or legal person;
d) The transfer is necessary for important reasons of public interest;
e) The transfer is necessary for the establishment, exercise or defense of legal claims; and
f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

DUCHESS, in compliance with the Regulation, shall explicitly communicate through clear warnings of the specific principle(s) of data protection that is/are likely to be violated in the event of a transfer to a third country.

8.11 Rights of Data Subjects

To comply with this section under the Regulation, DUCHESS shall:

a) 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, for any information addressed specifically to a child;
b) Provide such information in writing, or by other means, including, where appropriate, by electronic means;
c) Provide any information relating to processing of data obtained from the data subject orally, at the request of the data subject, provided that the identity of the data subject is proven by other means;
d) Inform the data subject without delay and at least within one month of receipt of a request relating to the processing of his/her data, the reasons for not providing the information and the possibility of lodging a complaint with the supervisory authority;
e) Provide information, any form of communication or any actions taken to a data subject free of charge;
f) Charge data subject if request for his/her data is manifestly unfounded or excessive, in particular because of his/her repetitive character. The charge shall be a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested;
g) Write a letter to the data subject stating "refusal act" on the request and copy NITDA on every occasion through a dedicated channel which shall be provided for such purpose, provided that such request is excessive;
h) Bear the burden of demonstrating the manifestly unfounded or excessive character of the request;
i) Request for provision of additional information necessary to confirm the identity of the data subject where DUCHESS has reasonable doubts concerning the identity of the requestor;
j) Provide the information 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 and machine-readable format when presented electronically;
k) Provide the data subject with all the following information, prior to collecting personal data:
    - The identity and the contact details of DUCHESS,
    - The contact details of the Data Protection Officer,
    - The purposes of the processing for which the personal data are intended as well as the legal basis for the processing,
    - The legitimate interests pursued by DUCHESS or by a third party,
    - The recipients or categories of recipients of the personal data, if any,
    - Where applicable, the fact that DUCHESS intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by NITDA,
    - The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,
    - The existence of the right to request from DUCHESS, 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,
    - The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal,

- The right to lodge a complaint with a relevant authority,
- 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,
- 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 data subject,
- Where DUCHESS intends to further process the personal data for a purpose other than that for which the personal data were collected, DUCHESS shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information, and
- Where applicable, that DUCHESS 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;

l) Inform the data subject the appropriate safeguards for data protection in the foreign country;

m) Rectify, without undue delay, inaccurate personal data concerning data subjects per their requests;

n) Acknowledge the right of data subjects to have their incomplete data completed, including by means of providing a supplementary statement;

o) Delete personal data without delay, upon request of the data subject;

p) Delete personal data where one of the following grounds applies:
   - The personal data are no longer necessary in relation to the purposes for which they were collected or processed,
   - The data subject withdraws consent on which the processing is based,
   - The data subject objects to the processing and there are no overriding legitimate grounds for the processing,
   - The personal data have been unlawfully processed, and
   - The personal data shall be erased for compliance with a legal obligation in Nigeria;

q) Take all reasonable steps to delete all the personal data made public and inform other companies processing the personal data of the data subject request;

r) Acknowledge data subjects' rights to obtain restriction of processing their personal data where one of the following applies:
   - The accuracy of the personal data is contested by the data subject for a period enabling DUCHESS to verify the accuracy of the personal data,
   - The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,
   - DUCHESS 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
   - The data subject has objected to processing pending the verification to confirm whether the legitimate grounds of DUCHESS override those of the data subject;

s) Process personal data with the data subject consent, where processing has been restricted;

t) Communicate any rectification or erasure of personal data or restriction to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort;

u) Provide personal data concerning data subjects, in a structured manner, commonly used and machine-readable format to such data subjects;

v) Not hinder the data subject from transmitting those data in its database to another company where the processing is based on consent, on a contract and processing is carried out by automated means; and

w) Execute data subjects' requests on transmission of their personal data to another company, where technically feasible.

9. ROLES & RESPONSIBILITIES

In compliance with the Regulation, DUCHESS has identified key stakeholders and their responsibilities to drive the operationalisation of the Policy and implementation of necessary data protection controls.

9.1 Board

a) Set the tone at the top on data protection; and
b) Ultimately responsible for ensuring that DUCHESS meets the obligations of the Regulation.

9.2 Executive Management Committee

a) Ensure data protection objectives are established and are aligned with the strategic direction of DUCHESS;
b) Ensure that the resources needed for the protection of data are available;
c) Communicate the importance of effective data protection in DUCHESS and of conforming to its requirements; and
d) Support other relevant Management roles to demonstrate their leadership as it applies to their areas of responsibility.

9.3 Chief Risk Officer

a) Approve any data protection statements attached to communications such as emails and letters;
b) Approve any data protection queries from journalist or media outlets such as newspaper;
c) Provide directives that ensures marketing initiatives abide by data protection principles;
d) Work with Marketing and Corporate Communication (MCC) department to address any data protection queries from journalists or media outlets in general; and
e) Work with MCC to ensure marketing initiatives abide by data protection principles.

9.4 Chief Information Officer

a) Evaluate any third-party services DUCHESS is considering using to store or process data such as private cloud computing services;
b) Responsible for assembling IT teams in the event of disaster;
c) Responsible for ensuring that security patches and bug fixes (vulnerabilities) are updated and kept current for servers/systems/devices under their control; and

d) Responsible for ensuring that virus protection software and signature files are updated and kept current for servers/systems/devices under their control.

9.5 Data Protection Officer

a) Create regular awareness (Data Protection relating trainings and education) to ensure that users are aware of this policy;
b) Ensure that this policy is published using approved channels;
c) Ensure the effectiveness of this policy is adequate;
d) Provides updates to the Executive Management about data protection responsibilities, risks and issues;
e) Review all data protection procedures and related policies, in line with an agreed schedule;
f) Handle data protection questions from staff and any other individuals covered by this policy; and
g) Deal with requests from individuals to see the data DUCHESS holds about them (also termed a 'subject access request').

9.6 Information Security Unit

a) Perform regular checks and vulnerability scans to ensure adequate security of hardware and software used in data processing;
b) Collaborate with the IT team to ensure prompt closure of identified gaps and vulnerabilities from the scans across all systems;
c) Where appropriate, coordinate the engagement of external and approved consultants to conduct relevant data audits and other reviews to ensure compliance with this Policy and the Regulation;
d) Ensure all systems, services and equipment used for storing data meet acceptable security standards;
e) Carry out appropriate education, awareness and training on matters relating to data protection and the Regulation across DUCHESS; and
f) Provide periodic reports on the findings of all reviews and scans to senior management and the Board.

9.7 Internal Control Unit

a) Provide reasonable assurance regarding the achievement of the operational objectives, such as the effectiveness and efficiency of the security controls

9.8 Internal Audit Unit

a) Carry out internal audit and report findings to Executive Management and the Board; and
b) Recommend preventive and corrective action.

9.9 All Staff

a) Ensures that this policy is adopted within their area of responsibility;
b) Employees should keep all data secure, by taking sensible precautions and following laid down standards;

c) Personal data must not be disclosed to unauthorized people, either within DUCHESS or externally; and
d) Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

10. POLICY REVIEW

These Policy shall be subjected to annual review or whenever there are major changes that could impact on the objectives of the Data Protection

11. CONSEQUENCES

The consequence of not adhering to the Policy will be handled in line with DUCHESS Disciplinary Process & Sanctions Policy.

a. General Information

Title	Data Privacy and Protection Policy
Status	Mandatory
Issuing Department	Legal and Compliance
Distribution/Target Audience	All patients, vendors, suppliers and employees, including contracted staff of the DUCHESS International Hospital.
Approver	Management of the DUCHESS International Hospital.
Effective Date	
Version	1.0

b. Version Control

Version	Last Updated	Reason for Amendment
1.0		