TAPROBANE MEDICAL CENTER

Data Protection Policy

RC1217632

Last Updated September 2020

DEFINITIONS

TMC	Taprobane Medical Center, Abuja
NDPR	Nigeria Data Protection Regulation.
DPO	Data Protection Officer, James Akapo
EMR	Electronic Medical Register of client's records in which personal data is processed by TMC
Data Subject	A person identifiable by a hospital number on the EMR
Third party	Anyone/party who is not the data subject (or someone authorized by them) and not a TMC authorized staff or administrator.

1. Data protection principles

TMC, is committed to processing data in accordance with its responsibilities under the NDPR.

Part 2.1 of the NDPR requires that 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. A further processing may be done only for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

   ii. Any person or entity carrying out or purporting to carry out data processing under the provision of this paragraph (b) shall not transfer any personal data to any third party.

b. Adequate, accurate and without prejudice to the dignity of human person

c. Stored only for the period within which it is reasonably needed

d. Secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire, or exposure to other natural elements.

2. General provisions

a. This policy applies to all personal data processed by TMC.
b. The DPO shall take responsibility for TMC's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

d. TMC shall submit an audit of our privacy practices to the NITDA once our clients exceed 1000 within 6 months or if we process data of clients larger than 2000 within a year.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, TMC shall maintain an Electronic Medical Register of client's records.
b. The EMR shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to TMC shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by TMC must be done on lawful basis as stipulated by the NDPR.
b. TMC shall note the appropriate lawful basis in the EMR.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in TMC's systems.

5. Data minimisation

a. TMC shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. TMC shall take reasonable steps to ensure personal data is accurate to the best of our ability.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, TMC shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. TMC shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration,

unauthorised disclosure of, or access to, personal data, TMC shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the NITDA.

END OF POLICY