CAREPAY DATA PRIVACY AND PROTECTION POLICY

Table of Contents

1 Introduction

1.1 Objective and Scope

This document applies to both CarePay International and CarePay Limited (jointly referred to as "CarePay"). This document describes how CarePay protects the rights and privacy of its clients, staff and partners with regard to the data that it collects, handles and stores. The policy applies to everyone who has access toCarePay's systems and information. Any breach to the data privacy policy is considered an offence and in that case there is the possibility of disciplinary measures. This document has been developed to ensure that CarePay complies with data protection law and follows good practice, protects the rights of staff, customers and partners, is open about how it stores and processes data, and protects itself, clients, staff, and partners from the risks of data breach.

1.2 Target Audience

This document applies to all CarePay internal and external employees, full time equivalents, service providers and stakeholders including those governing, providing and receiving Information Technology services, at CarePay International, as well as CarePay country offices (including but not limited to Kenya and Nigeria). The target audience has to be aware of the content in this policy.

1.3 Legal basis

This document has been developed in accordance with international and national regulations, including but not limited to the General Data Protection Regulation (GDPR) 2018, Article 31 of the Kenyan constitution, and Chapter 23 Section 37 of the Constitution of the Federal Republic of Nigeria (Promulgation) Act.

2 Data Protection Principles

CarePay has adopted the following principles in accordance of the GDPR to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

2.1 Principle 1: Fair and Transparent processing of Data

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. CarePay shall;

- Ensure the Data Subject is aware of what processing shall occur (transparency)
- The Processing shall match the description given to the Data Subject (fairness)
- Data shall only be processed for one of the purposes specified

2.2 Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. CarePay shall specify exactly what the Personal Data collected shall be used for and limit the processing of that Personal Data to only what is necessary to meet the specified purpose.

2.3 Principle 3: Data minimization

Personal data should me adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

2.4 Principle 4: Accuracy

Personal Data shall be accurate and kept up to date. CarePay shall have in place processes for identifying and addressing out-of-date, incorrect and redundant data.

2.5 Principle 5: Storage Limitation

Personal data will not be stored for longer than the purposes of the processing of data require.

2.6 Principle 6: Integrity & Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing, and against accidental loss, destruction or damage. CarePay shall use appropriate technical and organizational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

2.7 Principle 7: Accountability

The Data Protection Officer shall be responsible for, and be able to demonstrate compliance with, the management of data in accordance with CarePay's Data Privacy and Protection Policy. CarePay must demonstrate that the principles (outlined above) are met for all personal Data for which it is responsible.

3 Responsibility

Everyone who works for or with CarePay has some responsibility for ensuring that data is collected, stored and handled appropriately and secure. The Data Protection Officer shall have overall responsibility over this policy and shall oversee its implementation.

3.1 Responsibilities of the data protection officer

The roles and responsibilities of the data protection officer are as below;

- Keeping the board updated about data protection responsibilities, risks and issues
- Educating CarePay and its employees on important compliance requirements and their data privacy and protection responsibilities
- To provide advice where requested as regards the data protection impact assessment and monitor its performance
- Conducting audits to ensure compliance and address potential issues proactively
- Collaborating with the regulatory authorities
- Serving as the point of contact between CarePay and regulatory authorities
- Monitoring performance and providing advice on the impact of data protection efforts
- Interfacing with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures CarePay has put in place to protect their personal information

The DPO of CarePay may fulfill other tasks and duties, but CarePay will ensure that any such tasks and duties do not result in a conflict of interests.

3.2 Responsibilities of the Privacy Officer

The roles and responsibilities of the privacy officer are as below;

- Maintaining comprehensive records of all data processing activities conducted by CarePay, including the purpose of all processing activities, which must be made public on request
- Implementing data protection efforts and monitoring their performance
- Training staff involved in data processing on data privacy and protection and continual awareness
- Keeping the data protection officer updated about data protection risks and issues

3.3 Responsibilities of the chief technical officer

The responsibilities of the chief technical officer are as below;

- Ensuring all systems, services and equipment used for collecting, handling and storing data meet acceptable security standards

- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third party services the company is considering using to store or process data
- Ensuring that privacy by design and privacy by default are considered in new products and processes.

3.4 Responsibilities of the product owners

The responsibilities of the product owners are as below;

- Ensuring all products adhere to the CarePay data privacy and protection policy and the GDPR
- Approving any data privacy and protection clauses associated with communications and consent within the products
- Ensuring partnership agreements adhere to the CarePay data privacy and protection policy
- Recording details of data processing activities associated with products, including the purpose of all processing activities, to share with the DPO
- Ensuring that privacy by design and privacy by default are considered in new products and processes.

3.5 Responsibilities of the marketing manager

The responsibilities of the marketing manager are as below;

- Approving any data protection statements attached to communications
- Addressing any data protection queries from journalists or media outlets
- Where necessary, working with other staff to ensure marketing initiatives are conducted in accordance with CarePay's data protection and privacy policy

3.6 All employees

The responsibilities of all employees are as below;

- All employees need to be aware of this policy and the privacy procedures and must act accordingly
- Employees need to inform the DPO in case of data breaches
- Employees must comply with the confidentially agreement

4 Purposes

CarePay works as an intermediary between healthcare care payers on the one hand and healthcare providers (independent processing managers) on the other.

CarePay registers beneficiaries (individuals) on the platform. CarePay pays the healthcare care providers for treatments received by a beneficiary, using funds that the beneficiary is entitled to, including personal savings accounts, donor funds, corporate funds, or insurance funds. In order to be able to

make payments to healthcare providers, CarePay must investigate whether the treatment has been carried out, whether the treatment is appropriate in light of the diagnosis and previous care given to the beneficiary, and whether the beneficiary concerned is entitled to funds (e.g., personal savings account funds, donor funds, corporate funds, insurance funds) that cover this treatment. CarePay must account for the use of the funds.

Purposes for which CarePay has processed personal data:

- Managing funds of those with personal savings accounts.
- Payment of care providers from funds to which a beneficiary is entitled (including personal savings account funds, donor funds, corporate funds, insurance funds).
- Using funds to finance care for specific target groups.
- Checking whether payments to care providers are justified.
- Account to regulators, lenders and healthcare payers (including donors, corporates, insurance companies and social insurance organizations).
- Linking the parties involved to healthcare providers.

5 Lawful basis of processing

CarePay shall process personal data fairly and lawfully in accordance with individuals' rights. CarePay, UAP and Safaricom are joint data controllers under GDPR. The legal ground for processing personal data for the purposes mentioned hereunder is the underlying agreement (contract) the customer agrees to when registering for the service rendered by UAP and CarePay through the M-TIBA platform. CarePay owns and administers the M-TIBA platform. When data subjects agree to the General terms and conditions of M-TIBA it also means that they agree to have their personal data processed for these purposes and in these manners. The data subjects are informed about their personal data being processed through these terms and conditions. -

6 Personal Data Collected

6.1 Employees

While using CarePay applications, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information may include, but is not limited to your name, your telephone number, your date of birth ("Personal Information").

6.2 Beneficiaries

Personal Data can be collected from the data subject or from third parties. The data is collected from the data subject when they make use of the M-TIBA platform

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- In country law expressly provides for the collection, processing or transfer of Personal Data.

7 Special categories of Personal Data

CarePay needs to process health (medical) data for the purpose of administering the M-TIBA platform. In order to process health claims from healthcare providers, CarePay needs health (medical) data to assess claims. CarePay aims for data minimization and processes no more than its intended purpose.

8 Data Security

Personal data must be kept secure against possible loss or misuse, The DPO shall establish data security procedures to ensure data is securely processed. The minimum set of technical and organizational security measures to be adopted by CarePay is provided in the CarePay 'Information Security Policy' and Information Security Management System.

9 Data Retention

Personal data collected will not be held for a longer period than necessary. The reasons the data was collected will be taken into account, as will any legal and contractual requirements. All Personal Data shall be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it. CarePay has described the data retention in a policy. It also describes how CarePay maintains this policy.

10 Global data transfer

Personal data will not be transferred to any other region with a lower level of data protection under Kenyan law.

11 Data subject rights

The DPO shall establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.

- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, CarePay shall consider each such request in accordance with all applicable laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

12 Consent

Much of the data collected and processed by CarePay is necessary for the performance of a contract between CarePay and the data subject. Some of the data collected by CarePay is subject to active consent by the data subject, separate from a contract. For this latter category of data, the subject may revoke their consent at any given time.. CarePayshall establish a system for obtaining and documenting Data Subject Consent for the collection, processing, and/or transfer of their Personal Data. The system must include provisions for:

- Informing the data subject in order to obtain valid consent
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given
- Documenting the given consents of the data subject
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

13 Data Audit Reviews

Regular internal and external data audits to manage and mitigate risks will be undertaken and recorded. These contain information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. CarePay strives to be certified for privacy and information security.

14 Processors

In the case of processing by external parties, involving data processing of personal data, CarePay makes agreements about the requirements that the processing must meet. These agreements comply with the law. CarePay checks these agreements at least once a year. When appointing a processor, a processor

agreement is concluded. This agreement shall be concluded in accordance with the working method laid down for processing agreements.

15 Data Breaches

All members of staff and partners are required to report data breaches to the DPO as soon as they become aware of them. A personal data breach has to be notified within 72 hours to the supervisory authority, so the sooner the DPO knows about it, the better. The DPO will ensure that all affected individuals are notified without undue delay.

The notification has to contain the following information regarding the breach which are therefore required to be communicated to the DPO as soon as possible

- the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

CarePay has made agreements with its processors in the processor agreements about data breaches. These agreements on data breaches are in line with the text above.

16 Data Protection by Design

CarePay will include data protection and privacy from the outset of designing its systems and products. CarePay meets the requirement of the GDPR of privacy by design and privacy by default. In order to do so, Carepay performs Data Protection Impact Assessments (DPIA's) when necessary.

17 Changes to This Privacy Policy

This Data Privacy and Protection Policy is effective as of <date> will remain in effect except with respect to any changes in its provisions in the future.

CarePay reserves the right to update or change this Data Privacy and Protection Policy at any time and this will be checked periodically. CarePay will regularly review its Data Privacy and Protection Policy and activities to ensure that they are up to date with the latest regulations as well as the latest technology innovations.

If any material changes are made to this Policy, we will notify clients, staff and partners either through email, or by placing a prominent notice on our internal and external website.

18 Training

All care pay staff are required to be adequately trained on this policy. New joiners will be trained on this as part of the induction process. Further training will be provided whenever there is a significant change to this policy. CarePay continuously pays attention to a number of important privacy topics. In this way, employees are aware and competent how they should handle personal data safely during their work.

The training will cover;

- Our data privacy and protection policies and procedures
- Laws relating to privacy.

19 Governance

The management board of Carepay states that they approved and support this underlying privacy and data policy. The management board considers it as important that employees adhere this policy. Compliance with legislation and regulations is part of the evaluation cycle with employees.

20 Appendix

20.1 Terms and Definitions

Term	Definition
Consent	Freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data
Data	Data means information which – (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or (e) Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)?
Privacy Officer (PO)	Privacy officers are officers responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

Data Protection Officer (DPO)	Data Protection Officer is an internal regulator and supervisor for data protection strategy in the organization.
Data Subject	Data subject is the individual whom particular personal data is about
Encryption	The process of coding information so that its content is not understandable to anyone who obtains the information. To read the information, an algorithm is required to restore the information to its original form. Information also may be one-way encrypted so that it is not possible to restore the information to its original form. One-way encryption typically is used to protect passwords while they are stored in computer memory.
Enterprise	Any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.
Personal Data	Personal data means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Personal Data Breach	This is a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This means that a breach is more than just losing personal data
Privacy	The right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed
Privacy Impact Assessment	A tool used to identify and reduce the privacy risks of entities by analyzing the personal data that are processed and the policies in place to protect the data
Recipient	Recipient, in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Special category personal data	This means personal data consisting of information as to - (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
Third Party	Third party means any person other than – (a) the data subject, (b) the data controller, or (c) Any data processor or other person authorized to process data for the data controller or processor.

20.2 Document Management

20.2.1 Document Revision Log

Date	Editor	Version #	Description of Change
Month Day Year	KPMG	1.0	Initial version.

20.2.2 Document Approvers

Approver Name	Signature	Date