REDEEMERS HEALTH VILLAGE

Human Resources Department

DATA PROTECTION & PRIVACY POLICY (NDPA 2023)

Policy Code: HR-POL-029

Date of Issue:	April 28, 2026	**Next Review Date:**	April 28, 2027
Version:	1.0	**Last Review Date:**	N/A — New Policy
Author:	Adedayo Bazunu, Acting Chief Human Resources Officer		
Directorate:	Human Resources Department		
Approved By:	Chief Executive Officer | REMCO, RHV Board		
Date Approved:	—		

Relevant Standards

- Nigeria Data Protection Act (NDPA) 2023
- Nigeria Data Protection Regulation (NDPR) 2019
- National Information Technology Development Agency (NITDA) Guidelines
- Nigeria Data Protection Commission (NDPC) Frameworks and Directives
- Labour Act of Nigeria (Cap L1 LFN 2004)
- RHV Code of Professional Conduct (HR-POL-028)
- RHV Whistleblowing & Protected Disclosure Policy (HR-POL-026)

Amendment History

Issue	Status	Date	Reason for Change	Authorised
1	Draft	April 28, 2026	New Policy — Board Submission	CHRO
2				
3				

1. Purpose

Redeemers Health Village (RHV) collects, processes, stores, and shares large volumes of personal data in the ordinary course of delivering healthcare and managing its workforce. This includes some of the most sensitive categories of personal data that exist — patients' health records, clinical histories, and medical diagnoses — as well as employees' personal and employment information.

This policy establishes RHV's framework for the lawful, fair, transparent, and secure handling of all personal data, in full compliance with the Nigeria Data Protection Act (NDPA) 2023 and all applicable guidelines issued by the Nigeria Data Protection Commission (NDPC). It defines RHV's obligations as a data controller, the rights of data subjects, and the responsibilities of every employee who handles personal data in the course of their duties.

Data protection at RHV is not a compliance exercise — it is a fundamental expression of our respect for the dignity and privacy of every patient and employee.

2. Scope

This policy applies to all personal data processed by RHV, including:

- Patient data — including clinical, diagnostic, treatment, billing, and contact information
- Employee data — including employment records, payroll, health information, performance, and disciplinary records
- Supplier and third-party data — including contact information and contractual details
- Visitor and third-party data collected on RHV premises

It applies to all employees, contractors, volunteers, students, and any other person who handles personal data on RHV's behalf, in any format — electronic, paper, verbal, or otherwise.

3. Definitions

Personal Data

Any information relating to an identified or identifiable natural person — a 'data subject'. This includes names, contact details, identification numbers, health information, financial data, images, or any combination of information that can identify a person.

Sensitive (Special Category) Personal Data

A subset of personal data that attracts a higher level of protection under the NDPA 2023 due to the particular risks its disclosure creates. At RHV, the most common categories include: health and medical data; biometric data; genetic data; religious beliefs; and data relating to criminal convictions. Processing of sensitive data requires additional justification and safeguards.

Data Controller

RHV is a data controller — the entity that determines the purposes and means of processing personal data. As data controller, RHV bears primary legal responsibility for compliance with the NDPA 2023.

Data Processor

Any third party that processes personal data on RHV's behalf — such as a laboratory information system provider, payroll processor, or cloud storage vendor. RHV remains responsible for ensuring that all data processors are bound by appropriate data processing agreements.

Processing

Any operation performed on personal data, including: collection, recording, storage, use, access, disclosure, transfer, and destruction.

4. Data Protection Principles

All personal data processed by RHV must comply with the following principles, which reflect the requirements of the NDPA 2023:

- Lawfulness, Fairness, and Transparency: Data is processed on a lawful basis, fairly, and in a manner transparent to the data subject.
- Purpose Limitation: Data is collected for specified, explicit, and legitimate purposes and not processed in any manner incompatible with those purposes.
- Data Minimisation: Only data that is adequate, relevant, and necessary for the stated purpose is collected and processed.
- Accuracy: Personal data is kept accurate and up to date. Inaccurate data is corrected or erased without delay.
- Storage Limitation: Data is kept only for as long as necessary for the purpose for which it was collected, or as required by law. After this period, it is securely destroyed.
- Integrity and Confidentiality (Security): Data is processed in a manner that ensures appropriate security, including protection against unauthorised access, loss, destruction, or damage.
- Accountability: RHV demonstrates compliance with these principles and is accountable to data subjects, the NDPC, and the public for how it handles personal data.

5. Lawful Basis for Processing

RHV will only process personal data where it has a lawful basis to do so under the NDPA 2023. The primary lawful bases relied upon by RHV are:

5.1 For Patient Data

- Provision of healthcare: Processing is necessary for the provision of preventive, diagnostic, or therapeutic medical services. This is the primary lawful basis for processing patient health data.
- Vital interests: Processing is necessary to protect the life of the data subject or another person in an emergency.
- Legal obligation: Processing is required to comply with a legal obligation (e.g., mandatory disease reporting to NCDC).
- Consent: Where no other basis applies, we will obtain the patient's explicit informed consent before processing their data.

5.2 For Employee Data

- Contract: Processing is necessary for the performance of the employment contract.
- Legal obligation: Processing is required by Nigerian employment, tax, pension, or labour law.
- Legitimate interests: Processing is necessary for RHV's legitimate operational interests, provided these are not outweighed by the employee's privacy rights.
- Consent: For processing beyond the above (e.g., use of an employee's image in RHV marketing), explicit consent is obtained.

6. Patient Data — Specific Obligations

Patient data is among the most sensitive and strictly regulated data that RHV handles. The following obligations are absolute:

- Patient data is accessed only by staff with a direct, legitimate clinical or administrative need in connection with that patient's care or the management of the care process.
- Patient records — electronic and paper — must be kept secure, accurate, and current at all times.

- Patient information must never be shared with family members, employers, insurance companies, media, or any third party without the patient's explicit consent, except where the law requires or permits disclosure (e.g., court order, statutory reporting obligation, imminent risk to life).
- Patient data must never be sent over unsecured channels (e.g., personal WhatsApp, personal email) under any circumstances.
- Paper patient records that are no longer required must be shredded using a cross-cut shredder; they may not be disposed of in general waste.
- Any suspected or confirmed breach of patient data must be reported to the Head of Department and HR within one (1) hour of discovery, and to the NDPC within 72 hours where required by the Act.

7. Employee Data — Specific Obligations

RHV processes employee data for the purposes of: recruitment and employment; payroll and statutory remittances; performance and career management; health and occupational safety; and legal compliance. The following obligations apply:

- Employee data is processed only for the purposes for which it was collected and is not used for any unrelated purpose without the employee's knowledge.
- Employees' health data (e.g., medical certificates, occupational health assessments) is stored separately from general HR files, with access restricted to authorised HR personnel only.
- Employee data is not shared with third parties (e.g., banks, government agencies, third-party service providers) without a lawful basis and appropriate data processing agreements.
- Employees have the right to access their own personal data held by RHV, request corrections to inaccurate data, and — in limited circumstances — request erasure or restriction of processing. Such requests must be submitted in writing to HR and will be responded to within 21 days.

8. Data Security Obligations for All Staff

Every employee who handles personal data bears personal responsibility for its security. All staff must:

- Access personal data only for purposes directly related to their legitimate work duties at RHV.
- Use only RHV-authorised systems, devices, and platforms for processing, storing, or transmitting personal data.
- Never share login credentials, access passwords, or authentication tokens with any other person.
- Lock their screen whenever they leave a workstation unattended, even briefly.
- Not remove personal data from RHV's systems or premises — electronically or physically — without written authorisation from their Head of Department.
- Not send personal data (especially patient data) by email without encryption, or through personal messaging applications under any circumstances.
- Store paper documents containing personal data in a locked filing cabinet or secure location when not in immediate use.
- Report any lost or stolen device containing RHV data immediately to IT and HR.
- Complete all mandatory data protection training within the required timeframe.

9. Data Retention

Personal data is retained for only as long as necessary for the purpose for which it was collected, or as required by applicable Nigerian law. RHV maintains a Data Retention Schedule, approved by the CHRO and Finance Director, that specifies retention periods for each category of data. Key retention periods include:

- Patient medical records: A minimum of six (6) years from the date of the last entry, or until the patient's 18th birthday (whichever is later), in accordance with professional standards.
- Employee HR records: Seven (7) years following termination of employment, or as required by statute.
- Payroll and tax records: Seven (7) years as required by FIRS regulations.

- Recruitment records for unsuccessful candidates: Six (6) months from the date of rejection.

At the end of the applicable retention period, personal data must be securely and irreversibly destroyed in accordance with RHV's Data Destruction Procedure.

10. Third-Party Data Processors

Where RHV engages a third-party organisation to process personal data on its behalf (e.g., payroll bureau, laboratory information systems provider, cloud infrastructure provider), the following requirements apply:

- A written Data Processing Agreement (DPA) must be in place before any processing commences, binding the processor to NDPA 2023 compliance standards.
- RHV will conduct due diligence on the data protection practices of all significant data processors before engagement.
- Processors may only process RHV data in accordance with RHV's written instructions and may not use it for their own purposes.
- Processors must notify RHV of any data breach affecting RHV data within 24 hours of discovery.

11. Data Breach Response

A personal data breach is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All employees must report any suspected or confirmed breach immediately to their Head of Department and to HR. RHV's data breach response protocol is as follows:

1. Contain: Immediately take steps to stop the ongoing breach and prevent further data loss or exposure.
2. Report internally: The CHRO is notified within one (1) hour of discovery. The CHRO notifies the CEO immediately.
3. Assess: HR and IT jointly assess the scope, nature, and risk of the breach within 24 hours.
4. Notify the NDPC: Where the breach is likely to result in a risk to the rights and freedoms of data subjects, RHV will notify the Nigeria Data Protection Commission within 72 hours of becoming aware, as required by NDPA 2023.
5. Notify affected data subjects: Where the breach is likely to result in a high risk to data subjects, they will be notified without undue delay.
6. Document and review: All breaches are documented in RHV's Breach Register. Root cause analysis is conducted and remedial measures implemented to prevent recurrence.

12. Rights of Data Subjects

Under the NDPA 2023, individuals whose data RHV processes have the following rights, subject to applicable exemptions:

- Right of Access: To receive a copy of their personal data held by RHV.
- Right to Rectification: To have inaccurate data corrected.
- Right to Erasure: To have data deleted where it is no longer necessary, consent has been withdrawn, or processing is unlawful.
- Right to Restriction of Processing: To limit how their data is used in certain circumstances.
- Right to Data Portability: To receive their data in a structured, commonly used, machine-readable format.
- Right to Object: To object to processing based on legitimate interests or for direct marketing.

All data subject requests must be submitted in writing to the HR Department and will be addressed within 21 days. Where the request is complex or numerous, this period may be extended by up to a further 42 days, with written notice to the data subject.

13. Data Protection Officer

RHV designates the Acting Chief Human Resources Officer as its primary Data Protection contact, responsible for: advising on data protection obligations; monitoring compliance; serving as the point of contact with the NDPC; and maintaining RHV's data processing records. Where required by the NDPA 2023, RHV will appoint a formally designated Data Protection Officer (DPO), whose details will be published on the NDPC register.

14. Training and Compliance

All employees who handle personal data must complete mandatory data protection training as part of their induction and annually thereafter. Clinical staff and IT staff receive enhanced training appropriate to the volume and sensitivity of data they handle. Completion of training is recorded in the HR system. Non-compliance with data protection obligations by any employee will be treated as a serious disciplinary matter, up to and including dismissal where the breach involves patient data or is wilful in nature.

15. Monitoring and Review

The CHRO maintains RHV's Record of Processing Activities (ROPA) as required by the NDPA 2023. This policy, the Data Retention Schedule, and the ROPA are reviewed annually. Any changes to Nigerian data protection law or NDPC guidance will trigger an unscheduled review. The Board receives an annual data protection compliance report from the CHRO as part of its governance reporting.