

PRIVACY POLICY

Hospital Management Information System (HMIS) Provider

Document No.: PP-HMIS-001

Version: 1.0

Effective Date: 30/06/2026

Review Date: 30/06/2027

Policy Owner: Alphicons Investments Ltd.

1. Purpose

This Privacy Policy describes how **[Alphicons investments LTD]** (“the Company”, “we”, “our”, or “us”) collects, uses, processes, stores, secures, and discloses personal data while providing Hospital Management Information System (HMIS) software, cloud hosting, implementation, maintenance, integration, technical support, and related digital health services.

The Company is committed to protecting the privacy and confidentiality of personal data in accordance with the **Kenya Data Protection Act, 2019**, the **Data Protection (General) Regulations, 2021**, and other applicable laws and standards.

2. Our Role

Depending on the service provided, the Company may act as:

- **Data Processor** – where we process personal data solely on behalf of healthcare providers (our clients) and in accordance with their documented instructions.

Healthcare facilities using our HMIS remain responsible for determining the purposes and means of processing patient data where they act as Data Controllers.



ALPHICONS
INVESTMENTS LTD
Consulting Web & Technology
Custom Programming Company

3. Scope

This policy applies to:

- HMIS Software (Cloud and On-Premise)
 - Electronic Medical Records (EMR)
 - Patient Portals
 - Mobile Applications
 - Web Portals
 - Customer Support Services
 - API Integrations
 - SMS and Email Notification Services
 - System Monitoring
 - Software Updates
 - Training Services
 - Technical Support
 - Disaster Recovery Services
 - Backup Services
-

4. Personal Data We Process

A. Data Processed on Behalf of Clients

While providing HMIS services, we may process:

- Patient names
- National ID/Passport numbers
- Patient numbers
- Date of birth
- Gender
- Telephone numbers
- Email addresses
- Residential addresses
- Next of kin information
- Clinical notes
- Medical history



- Diagnoses
- Prescriptions
- Laboratory results
- Radiology reports
- Admission and discharge records
- Appointment information
- Insurance information
- Billing information
- Payment records
- Healthcare worker details
- User account information

Such data is processed only under the instructions of the healthcare facility that controls the data.

B. Company Business Data

We also process personal data relating to:

- Employees
 - Job applicants
 - Customers
 - Client representatives
 - Suppliers
 - Contractors
 - Website users
 - Training participants
 - Support contacts
-

5. Purposes of Processing

We process personal data for purposes including:

- Provision of HMIS software
- Software implementation
- System configuration

- User authentication
- Technical support
- Bug fixing
- Software maintenance
- System monitoring
- Database administration
- Performance optimization
- Backup management
- Disaster recovery
- Cybersecurity monitoring
- API integrations
- Customer relationship management
- Billing
- Contract management
- User training
- Product improvement
- Compliance with legal obligations

We do not process patient data for marketing purposes.

6. Legal Basis for Processing

Where acting as a Data Controller, we process personal data based on:

- Consent where required
- Contractual necessity
- Legal obligations
- Legitimate business interests
- Protection of vital interests
- Public interest where applicable

Where acting as a Data Processor, we process personal data only on documented instructions from our client unless otherwise required by law.

7. Confidentiality

All employees, consultants, developers, database administrators, system administrators, implementation engineers, and technical support staff are bound by confidentiality agreements and receive data protection training.

Access to customer data is granted strictly on a need-to-know basis.

8. Data Security

We implement appropriate technical and organizational security measures, including:

- Encryption of data in transit using TLS
 - Encryption of stored data where applicable
 - Role-based access control (RBAC)
 - Multi-factor authentication for privileged accounts
 - Strong password policies
 - Audit logging and monitoring
 - Secure software development practices
 - Vulnerability assessments and penetration testing
 - Endpoint protection
 - Firewalls and network segmentation
 - Secure backup and recovery procedures
 - Disaster recovery planning
 - Physical security for hosted infrastructure
 - Periodic security reviews
-

9. Data Sharing

We do not sell personal data.

Where necessary, personal data may be shared with:

- Cloud infrastructure providers
- SMS gateway providers
- Email service providers
- Payment processors
- Identity verification providers
- Integration partners
- Regulatory authorities
- Law enforcement agencies where legally required
- Independent auditors under confidentiality obligations

All third-party service providers are contractually required to implement appropriate data protection safeguards.

10. International Data Transfers

Where personal data is transferred outside Kenya, we ensure that appropriate safeguards are in place, including contractual protections and compliance with applicable legal requirements.

11. Data Retention

As a Data Processor, we retain personal data only for the period specified in our contract with the healthcare provider or as instructed by the client.

Company business records are retained in accordance with legal, regulatory, tax, and operational requirements.

Upon termination of services, client data is securely returned or deleted in accordance with contractual obligations.

12. Data Subject Rights

Where we act as a Data Controller, individuals may exercise the following rights:



- Right to be informed
- Right of access
- Right to correction
- Right to erasure where applicable
- Right to object to processing
- Right to restrict processing
- Right to data portability where applicable
- Right to withdraw consent where processing is based on consent

Where we act solely as a Data Processor, requests relating to patient data should ordinarily be directed to the relevant healthcare provider, although we will assist our clients in responding to such requests where required.

13. Cookies and Analytics

Our website and online services may use cookies and similar technologies to:

- Maintain secure user sessions
- Improve system performance
- Measure website usage
- Enhance user experience

Users may manage cookie preferences through their browser settings.

14. Data Breach Management

The Company maintains documented procedures for identifying, investigating, containing, mitigating, documenting, and reporting personal data breaches.

Where we become aware of a breach affecting client data, we will notify the relevant client without undue delay and cooperate with them in meeting any legal notification obligations.

15. Customer Responsibilities

Healthcare providers using our HMIS are responsible for:

- Obtaining any required patient consents
 - Maintaining accurate patient records
 - Managing user accounts and permissions
 - Reporting suspected security incidents
 - Complying with applicable data protection laws
 - Informing data subjects how their information is processed
-
-

16. Complaints

Questions or complaints regarding this Privacy Policy should be directed to the Company's Data Protection Officer.

Individuals also have the right to lodge a complaint with the Office of the Data Protection Commissioner (ODPC) in accordance with applicable law.

17. Policy Review

This Privacy Policy shall be reviewed at least once every twelve (12) months or whenever there are significant changes to legislation, technology, or the Company's services.



Approval

Approved by:

Managing Director: Stelon Shadrack Wambua

Signature:

A handwritten signature in black ink, appearing to read 'Stelon Shadrack Wambua', is written over a light blue horizontal line.

Date: 30/06/2026