

DHA CERTIFICATION · COMPLIANCE

Privacy Policy

MedX

Applicant	MedX Technologies Kenya Ltd
DHA application	APP-2026-AMY1EC
Document ID	MXK-DHA-01
Version	1.0
Date	October 2026
Owner	Anthony Ndolo, Managing Director
Classification	Public: published at https://medx.to/ke/privacy and submitted to the Digital Health Agency

Document control

Document ID	MXK-DHA-01
Version	1.0
Status	Approved for publication and submission
Published at	https://medx.to/ke/privacy
Review frequency	Annually, and whenever the way we process personal data or the law changes
Related documents	MXK-DHA-05 Information Security Policy; MXK-DHA-06 Incident Response Plan; MXK-DHA-14 Data Retention and Disposal Policy

Version	Date	Change	Author
1.0	October 2026	First issue	Anthony Ndolo

1. About this policy

This policy explains how MedX Technologies Kenya Ltd ("MedX Kenya", "we", "us") handles personal data in connection with our laboratory software in Kenya. It is written for:

- **patients** whose tests are processed by a laboratory, hospital or clinic that uses our software;
- **facility staff** who use our software at work;
- **customers and business contacts** of MedX Kenya.

Our software is MedX, a laboratory information system that laboratories use to register patients with their test requests, manage samples, record results and issue reports. In this policy, "the System" means MedX as deployed for a Kenyan laboratory, together with its identity service and its FHIR data store. The System processes patient data on behalf of the laboratories that use it.

MedX has two parts. The MedX web app is the application staff use in their browser, hosted in Kenya. MedX device connectivity runs at the laboratory itself, either as the MedX desktop app on a laboratory PC or on a MedX site server (a server MedX supplies and manages at larger laboratories). It receives results from the laboratory's analysers (the machines that run the tests) and passes them to the web app, where laboratory staff check and release them in the same way as results typed in by hand.

We follow the Data Protection Act, 2019 and the regulations made under it, and the Digital Health Act, 2023.

2. Who we are and our role

MedX Technologies Kenya Ltd is a company registered in Kenya, company number PVT-8Z1ZRZB8, registered office Woodvale, Woodvale Street, Westlands, Nairobi; P.O. Box 70423-00100 GPO Nairobi. MedX affiliates develop the software and provide second-line support under a services and data processing agreement with MedX Technologies Kenya Ltd.

We have two roles under the Data Protection Act, 2019:

- **For patient data we are a data processor.** The laboratory, hospital or clinic that tests you is the data controller: it decides what data is collected and why. We store and process the data in the System only on the facility's instructions, under a written contract. If you are a patient, your facility's own privacy notice also applies, and your facility is your first point of contact.
- **For our own business data we are a data controller.** This covers the user accounts of facility staff, and the details of our customers, business contacts and people who contact us.

We are registered with the Office of the Data Protection Commissioner (ODPC) as a data controller (registration 165-593B-D994, certificate no. 30174, valid 8 October 2026 to 8 October 2028) and as a data processor (registration 165-593B-D994, certificate no. 27507, valid 22 September 2026 to 22 September 2028).

3. What personal data we handle

About whom	Data
Patients (on behalf of the facility)	Identity and demographics: name, sex, date of birth or age, identifiers such as a facility patient number and National ID, Maisha Namba, birth certificate, passport, alien ID, Client Registry number or SHA number. Contact: phone number, email address, address (including county, sub-county and ward). Clinical and laboratory data: test requests, the requesting clinician, clinical information given with the request, samples, results, reports, comments, and payment records for the tests (amounts and receipts). Analysers data at the laboratory: MedX device connectivity keeps a short-term copy of each result it receives, the original message from the analyser, any patient details the analyser sends with the result (some analysers send a name, age or sex) and the list of tests waiting to be run on each sample. Health data is sensitive personal data under the Data Protection Act, 2019 and receives extra protection.
Facility staff (System users)	Name, work email and phone, role and permission level, facility, sign-in records, and a record of actions taken in the System (the audit trail). Passwords are stored only in a protected (hashed) form that cannot be read back.
Customers and business contacts	Name, organisation, job title, work contact details, contract and billing information, and support requests.
Technical data	IP address, browser and device type, and session information when you use the System. From MedX device connectivity, a health status report to the facility's web app: the app version, which analysers are connected, how many results are waiting and when the last result was delivered, with no patient data. We use this to run and secure the service.

4. Where the data comes from

- **Patient data** comes from the facility: from you at registration, from the request form completed by your clinician, from laboratory staff, from the facility's other systems (for example its electronic medical record) and from laboratory analysers. Analysers send results to MedX device connectivity at the laboratory, which links each result to your sample by the barcode on the sample label and passes it to the web app. Each analyser result is then checked by one member of laboratory staff and released by another, in the same way as a result typed in by hand; results are never released automatically. A result that cannot be matched

to a sample, or that arrives after the sample's result was released, is set aside for a laboratory technician to deal with, and a released result is never overwritten.

- **Staff user data** comes from the facility administrator who invites the member of staff, and from the user.
- **Business contact data** comes from you or your organisation.
- **Technical data** is generated when the System is used.

5. Why we use personal data, and our lawful basis

Purpose	Lawful basis
Providing laboratory services for patients on the facility's behalf: registration, requests, samples, results and reports.	We process on the facility's instructions. The facility relies on the provision of health care and the management of health services, and on the grounds for processing sensitive personal data for health purposes under the Data Protection Act, 2019, by or under the responsibility of health professionals bound by confidentiality.
Reporting notifiable diseases and weekly disease surveillance to public health authorities, where the law requires it.	Compliance with a legal obligation of the facility (Health Act, 2017 and the Kenya IDSR Technical Guidelines) and public interest in public health.
Providing and managing staff user accounts, keeping the audit trail, supporting users.	Performance of our contract with the facility, and our legitimate interest in running a secure, accountable service; legal obligations on the facility to keep records.
Keeping the System secure, preventing misuse, investigating incidents.	Legitimate interest and legal obligations on us and the facility to protect personal data.
Managing customer relationships, contracts, billing and support.	Performance of contract; legal obligations (for example tax records); legitimate interest.

We do not use patient data for marketing. We do not sell personal data. Only aggregated or de-identified data, which does not identify any patient, is used for service statistics or, where the facility agrees, research.

When you are registered, the facility records that you have been given its privacy notice and any consent it asks for.

6. Who we share data with

- **The facility** that holds your record, and its staff according to their role.
- **Clinicians and others the facility directs**, for example the clinician who requested your test, or a referral laboratory. The facility gives or sends your printed report to you or your clinician.
- **The national Health Information Exchange (Afya Connect)**, where the facility uses it: the System looks up and confirms your identity in the national client registry when you are registered, identifies the facility by its Kenya Master Health Facility List (KMHFL) code, and sends released laboratory results to your shared health record, on the facility's behalf.
- **Public health authorities**, where the law requires notifiable disease reporting and IDSR reporting: for example the facility's disease surveillance focal person, the sub-county and county disease surveillance

coordinators, and the Ministry of Health's Kenya Health Information System (KHIS). The System sends these alerts and weekly reports on the facility's behalf.

- **Our sub-processors**, who help us provide the service, each under a written agreement that requires them to protect the data and use it only for our instructions:
 - MedX affiliates: software development and second-line support, under a services and data processing agreement with MedX Kenya. Their engineers, who may be outside Kenya, can see patient data only during a support session that the facility approves (section 7);
 - Servercore (Nairobi, Kenya): hosting of the System in a Tier III data centre in Nairobi;
 - Angani Limited (Nairobi, Kenya): storage of encrypted backups at a second data centre in Nairobi;
 - Amazon Simple Email Service (Amazon Web Services, Cape Town region): delivery of account invitations, password resets and system notifications. Patient data in these emails is kept to the minimum needed;
 - Africa's Talking (Nairobi, Kenya): delivery of SMS notifiable disease alerts and result notifications.
- **Authorities** such as the ODPC, the Digital Health Agency, courts or the police, where the law requires us to.

Where the facility enables it, the System sends result notifications to patients and clinicians by SMS or email, with only the details needed to tell them a result is ready. We tell our customers before we add a new sub-processor.

7. Where the data is kept

Kenyan patient data is stored and processed in Kenya, on MedX-operated servers in the Servercore Nairobi region (a Tier III data centre in Nairobi operated by iColo/Digital Realty). Each facility's data is held in its own database. Backups are kept at a second, separate data centre in Nairobi, operated by Angani Limited.

The servers are administered by MedX Kenya staff based in Kenya. MedX engineers outside Kenya, including those of MedX affiliates, have no access to patient data by default. If a support case needs it, the facility's administrator can grant one named engineer a support session, linked to the support ticket, that lasts at most 4 hours, allows viewing only unless the administrator allows changes, and can be ended at any time. Everything done in the session is recorded in the facility's audit trail. No copy of Kenyan patient data is stored outside Kenya.

MedX device connectivity also keeps a short-term copy of analyser data at the laboratory, on the laboratory PC that runs the MedX desktop app or on the MedX site server. This copy is encrypted (AES-256), and only signed-in staff with the right permission level can view it. It is kept for 30 days after each result has been delivered to the web app, and is then deleted automatically (section 8). The web app remains the facility's record. Device connectivity sends data outside the laboratory only to the facility's own MedX web app (results and a health status report with no patient data) and to MedX's update service (to check for software updates, with no patient data). It sends nothing to analytics, crash reporting or location services.

To deliver account and notification emails, the recipient's email address and the message are passed to Amazon Simple Email Service in its Cape Town region (South Africa), under the provider's data processing terms and the safeguards required by the Data Protection Act, 2019. Patient data in email is kept to the minimum needed.

8. How long we keep data

The facility decides how long patient records are kept. Our default periods are below; records are kept for at least 7 years, or longer where Ministry of Health records guidance or the facility requires.

Data	Default retention
Patient records, requests, results and reports	At least 7 years after the last activity; for children, until age 25 or 7 years, whichever is later
Audit trail and sign-in records	7 years
Analyser graphs attached to results	The same as the result they belong to
Backups	Up to 7 years (yearly copies), shorter for daily and monthly copies
Staff user accounts	Disabled when the person leaves; the account record is kept for 7 years so that past actions remain attributable
Technical logs	90 days (security logs 1 year)
Analyser results and original analyser messages held at the laboratory by MedX device connectivity, including any patient details the analyser sends	Until delivered to the web app, then 30 days; then deleted automatically. A result that has not been delivered is never deleted, and the laboratory is alerted after 24 hours
Tests waiting to be run, sent to analysers by MedX device connectivity	Until the sample's result is delivered, or 7 days, whichever comes first
MedX device connectivity logs at the laboratory	7 days; they hold only sample numbers and counts, never patient names or results

Records under a legal hold are kept until the hold is released. At the end of the period data is securely deleted through an approved disposal process recorded in the audit trail.

9. How we protect data

We protect personal data with technical and organisational measures, including:

- access based on each user's role, checked on the server for every request and limited to their own facility, with individual accounts only;
- multi-factor authentication for staff who review and release results, administrators and all MedX staff;
- encryption of data in transit (TLS 1.3 on our public endpoints, and TLS 1.2 or higher on our connections to external services such as the Health Information Exchange, email and SMS providers) and encryption of stored data and backups (AES-256);
- an audit trail of who changed which record and what they changed, which also records who viewed records and cannot be altered;
- regular backups and monitoring, staff confidentiality agreements and training;
- independent security testing.

If a personal data breach affects patient data, we tell the facility within 24 hours of becoming aware of it and help it inform the ODPC and, where required, affected people.

10. Your rights

Under the Data Protection Act, 2019 you have the right to:

- **be informed** of how your personal data is used (this policy and the facility's notice);
- **access** the personal data held about you;
- **object** to the processing of all or part of your personal data;
- **have inaccurate or misleading data corrected**;
- **have false or misleading data deleted**, and data deleted where there is no longer a lawful reason to keep it;
- **data portability**: to receive your data in a structured, commonly used, machine-readable format and have it sent to another controller where technically possible;
- **restrict** processing in certain circumstances.

Some rights are limited by law. For example, laboratory records may need to be kept for your ongoing care or to meet health records rules even if you ask for deletion, and public health reporting required by law cannot be stopped by objection. We will explain if a right cannot be applied.

How to exercise your rights

- **Patients:** please contact the facility that tested you, because it controls your record. If you contact us, we will pass your request to the facility promptly and help it respond. The System lets the facility export your data, and it records every correction made to your details in the audit trail.
- **Facility staff, customers and business contacts:** contact our Data Protection Officer at privacy@medx.international.

We may ask you to confirm your identity before acting on a request. We acknowledge requests within 7 days and answer them within the period set by the Data Protection Act, 2019 and its regulations. There is normally no charge.

11. Children

Laboratories test children, so the System holds data about children on behalf of facilities. The facility is responsible for obtaining any consent needed from a parent or guardian and for giving them its privacy notice. A parent or guardian may exercise a child's rights through the facility. Records of children are kept for longer (section 8). We do not offer any service directly to children.

12. Cookies and similar technologies

MedX uses only session cookies that are strictly necessary to sign staff in and keep their session secure:

- a session cookie set by the facility's sign-in gateway (oauth2-proxy), which is valid only for that facility's own web address;
- the session cookies of our sign-in service (Keycloak), which end when the session ends.

We do not use advertising or analytics cookies, and the System contains no third-party analytics. The address field does not send what you type to a public mapping service. Patients do not use the System directly, so no cookies are set on patients' devices.

The MedX desktop app uses no cookies and no tracking. It stores its encrypted local copy (section 7) and its settings on the laboratory PC, and the key that protects that copy is held by the PC's operating system. The web interface of a MedX site server contains no tracking or analytics.

13. Automated decision-making

The System flags quantitative laboratory results that fall outside reference ranges for the patient's age, sex and sample type (high or low), and prints the laboratory's interpretation guide for each test on the report. It also alerts staff to critical results that need urgent attention. These flags support qualified laboratory staff and clinicians; results are reviewed and released by laboratory staff, and no decision that has a legal or similarly significant effect on you is made solely by automated means.

When a released result matches a condition that the law requires to be reported, the System alerts the facility's surveillance contacts so that they can follow up. This supports reporting that is required by law; it is not a decision about your care.

14. Complaints

If you are unhappy with how your data has been handled, please contact the facility (for patient records) or our Data Protection Officer. You also have the right to complain to the **Office of the Data Protection Commissioner** (ODPC), www.odpc.go.ke.

15. Changes to this policy

We review this policy at least once a year. If we make significant changes, we will publish the new version at <https://medx.to/ke/privacy> with its date and tell our customers. The version and date are shown at the top of this policy.

16. Contact us

Data Protection Officer	Anthony Ndolo, Managing Director, acting Data Protection Officer, MedX Technologies Kenya Ltd
Privacy requests	privacy@medx.international
Legal and Compliance	Anthony Ndolo, Managing Director, andolo@medx.international , +254 713 055784
Postal address	Woodvale, Woodvale Street, Westlands, Nairobi; P.O. Box 70423-00100 GPO Nairobi · Company No. PVT-8Z1ZRZB8 · KRA PIN P052567674Z
Phone	+254 713 055784
Support	support@medx.international · support.medx.to

17. Approval

Role	Name	Signature	Date
Prepared by	Anthony Ndolo, Managing Director		
Reviewed by	Ernest Okot, Technical Director		
Approved by	Anthony Ndolo, Managing Director		