AMCOA

ASSOCIATION OF MEDICAL COUNCILS OF AFRICA

RESPONSIVE REGULATION
FOR SAFER COMMUNITIES
TOWARDS UNIVERSAL HEALTH COVERAGE

28TH ANNUAL CONFERENCE

ACCRA, GHANA

23 – 27 AUGUST 2026

DEDICATED TO PROTECTING THE PUBLIC AND ADVANCING PROFESSIONAL STANDARDS IN AFRICA

Data Governance

Dr. David G. Kariuki
CEO and Registrar,
Kenya Medical Practitioners and Dentists Council

Data Governance

AMCOA

ASSOCIATION OF MEDICAL COUNCILS OF AFRICA

28TH ANNUAL CONFERENCE

ACCRA, GHANA

23 – 27 AUGUST 2026

MINISTRY OF HEALTH REPUBLIC OF GHANA

FREEDOM AND JUSTICE

MEDICAL AND DENTAL COUNCIL GHANA

One shared data layer can strengthen regulation across Africa

- Secure, standardized and timely exchange among healthcare regulatory authorities
- Faster, more transparent decisions that strengthen patient safety
- Regional integration and cooperation aligned with AfCFTA

Enablers are:

Interoperability • Governance • Cybersecurity • Mutual recognition

Data governance, cybersecurity and privacy

- Establish common data governance standards
- Ensure compliance with privacy and data protection laws
- Implement strong cybersecurity controls, access management, encryption and audit trails
- Build trust through accountability and secure data sharing

Why data governance matters for regulators

A

SENSITIVE
ACCOUNTABLE
TRUSTED

Regulators hold highly sensitive professional and institutional information.

- Practitioner identity and registration details
- Qualifications and training history
- Licences and practice status
- Disciplinary and professional-conduct records
- Health-facility registration and licensing information
- CPD records
- Examination and internship information

Cross-border exchange increases both risk and responsibility.

Data exchange must rest on trust, accountability and clearly defined rules — not simply technical connectivity.

Establish a common EAC regulatory data governance framework

B

DEFINE
ASSIGN
ACCOUNT

- **Data ownership —** who owns and controls the data?
- **Data stewardship —** who maintains its quality?
- **Data custodianship —** who stores and protects it?
- **Data access —** who may see or consume specific information?
- **Purpose limitation —** what may exchanged data legally be used for?
- **Data retention —** how long should information be retained?
- **Data-sharing agreements —** what obligations bind participating regulators?
- **Accountability —** who answers when data is wrong, misused or breached?

Build privacy into the infrastructure from the beginning

C

MINIMIZE
CONTROL
PROTECT

Privacy controls should be designed in — not added after deployment.

- Collect and exchange only the minimum data required
- Apply role-based access controls
- Encrypt data in transit and at rest
- Maintain comprehensive audit trails
- Authenticate every organisation and user accessing the platform
- Separate personally identifiable information from safely shareable data
- Establish data-breach notification and response procedures

Cross-border protection needs a shared regional baseline

D

ALIGN
PROTECT
ALLOW

NATIONAL VARIATION

- Different data-protection laws
- Different regulatory mandates
- Different definitions of sensitive data
- Different localisation and cross-border-transfer requirements

EAC DESIGN PRINCIPLE

Set a minimum common privacy and security standard

Apply it across the regional infrastructure while allowing each Member State to maintain stronger national requirements.

Data quality is part of governance

E

DEFINE
VALIDATE
TRACE

“Bad data exchanged efficiently is still bad regulatory data.”

THE FRAMEWORK SHOULD ESTABLISH

- Common data definitions
- Mandatory fields
- Validation rules
- Unique identifiers
- Data-quality standards
- Procedures for correcting erroneous records
- Data provenance — where information originated and when it was last updated

Create an EAC Regulatory Data Trust Framework

F

GOVERN
MONITOR
RESOLVE

A shared trust framework should define ten core components.

1. Common governance principles
2. Institutional roles and responsibilities
3. Authentication and identity management
4. Data classification
5. Privacy requirements
6. Cybersecurity standards
7. Data-sharing agreements
8. Audit and monitoring
9. Incident management
10. Dispute-resolution mechanisms

Cross-border information sharing and mutual recognition

04

SHARE
RECOGNIZE
RESPOND

- Enable secure exchange of licensing and regulatory information
- Support mutual recognition of regulatory decisions where appropriate
- Facilitate workforce mobility and coordinated public health responses
- Strengthen regional regulatory harmonization

Practical recommendations for Africa's digital regulatory infrastructure

05

STANDARDIZE
PILOT
SCALE

- **Develop continent-wide** interoperability standards and common data models
- **Establish** multi-country governance with clear roles, accountability and decision rights
- **Embed privacy-by-design**, cybersecurity, identity and access controls, and auditability
- **Pilot high-**value use cases in willing regions, then scale through mutual-recognition mechanisms
- **Invest in infrastructure**, workforce capability and sustainable funding