

# AMCOA

ASSOCIATION OF MEDICAL COUNCILS OF AFRICA



RESPONSIVE REGULATION  
FOR SAFER COMMUNITIES  
TOWARDS UNIVERSAL HEALTH COVERAGE

28<sup>TH</sup>  
ANNUAL  
CONFERENCE

ACCRA, GHANA

23 – 27 AUGUST 2026

DEDICATED TO PROTECTING THE PUBLIC AND ADVANCING PROFESSIONAL STANDARDS IN AFRICA

## Database Architecture

Dr. David Mnzava



# Connected Data, Trusted Regulation, Safer Healthcare Across Africa

**AMCOA**

ASSOCIATION OF MEDICAL COUNCILS OF AFRICA



# Outline

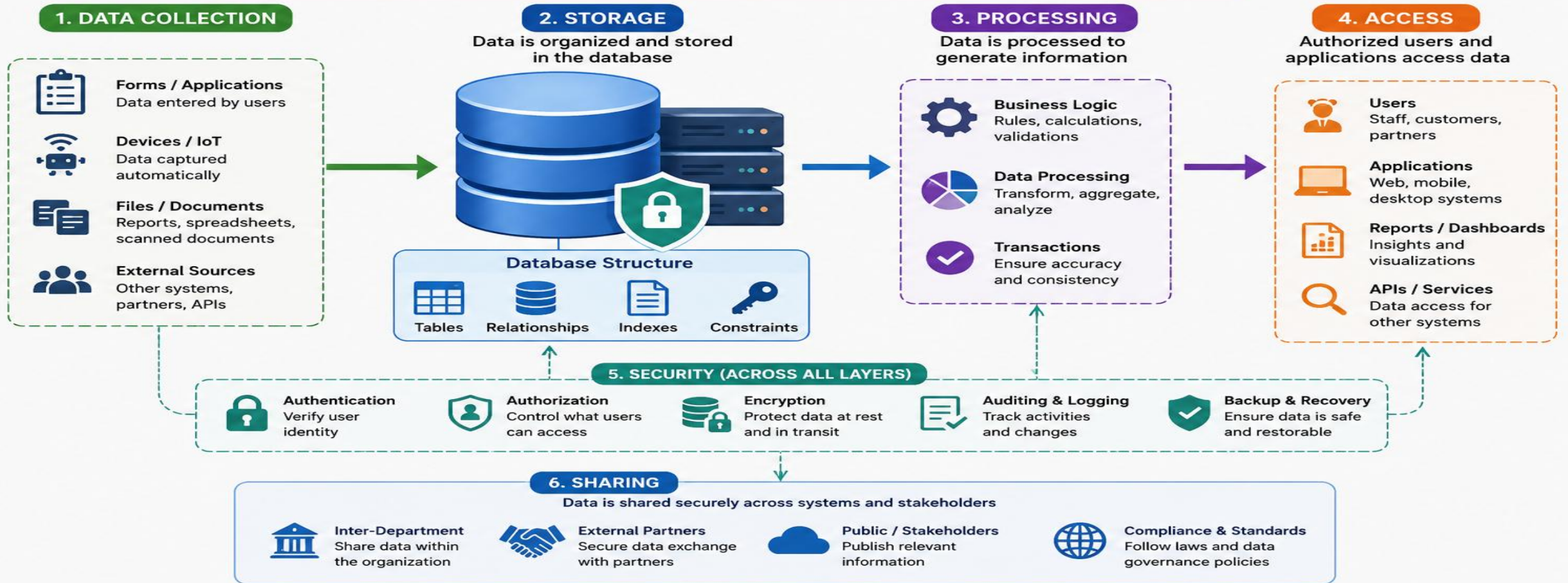
- What is Database architecture
- Evolution
- Programming language
- Minimum dataset requirement
- Core database component
- Security architecture
- Available technology opportunities
- AI in Regulatory Databases
- Migration from MCTIS to HPRS-Tanzania Examples



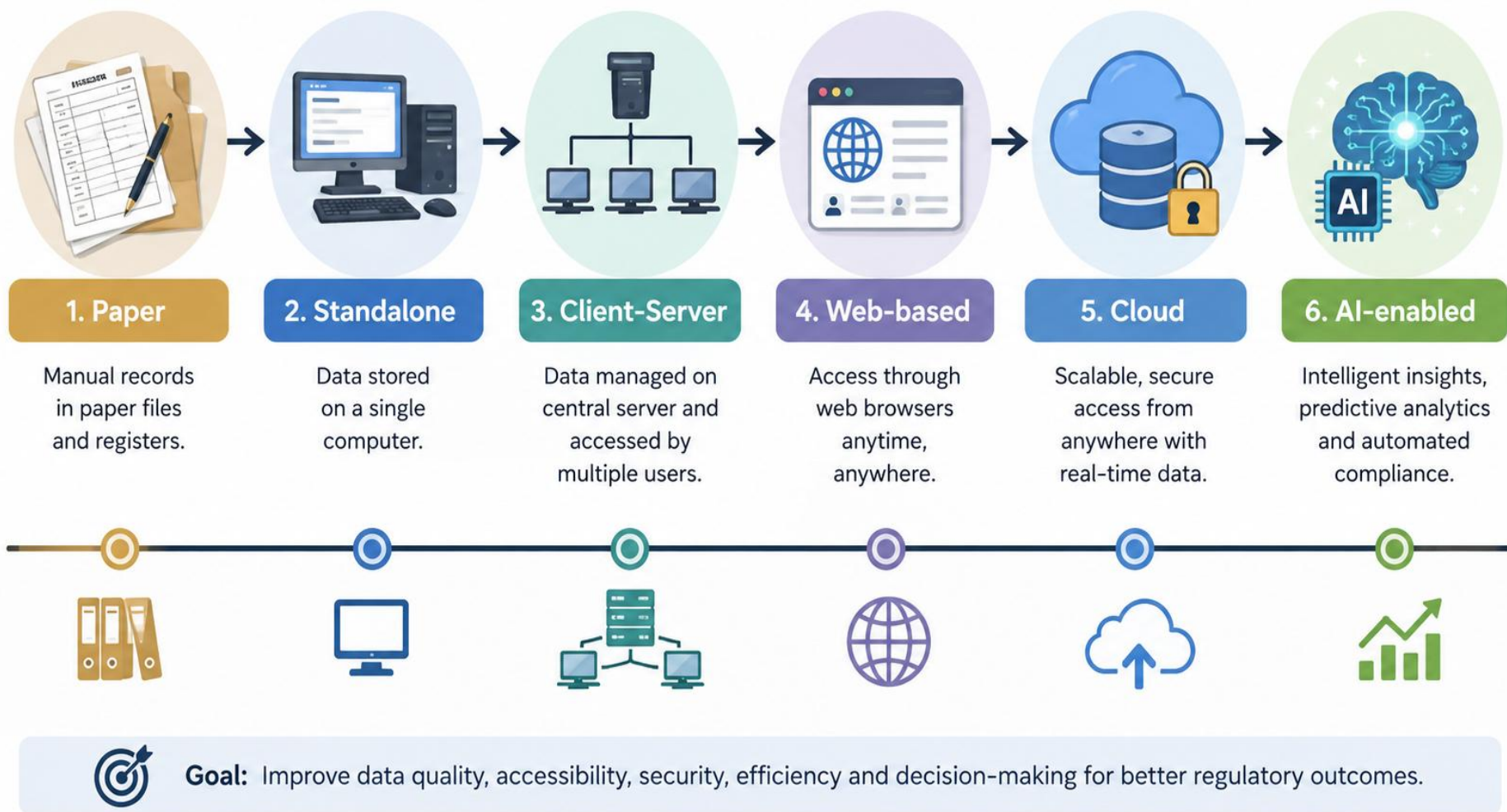
# DATABASE ARCHITECTURE



Database architecture is the structure and design of a system that determines how data is collected, stored, processed, secured, accessed, and shared across applications and users.



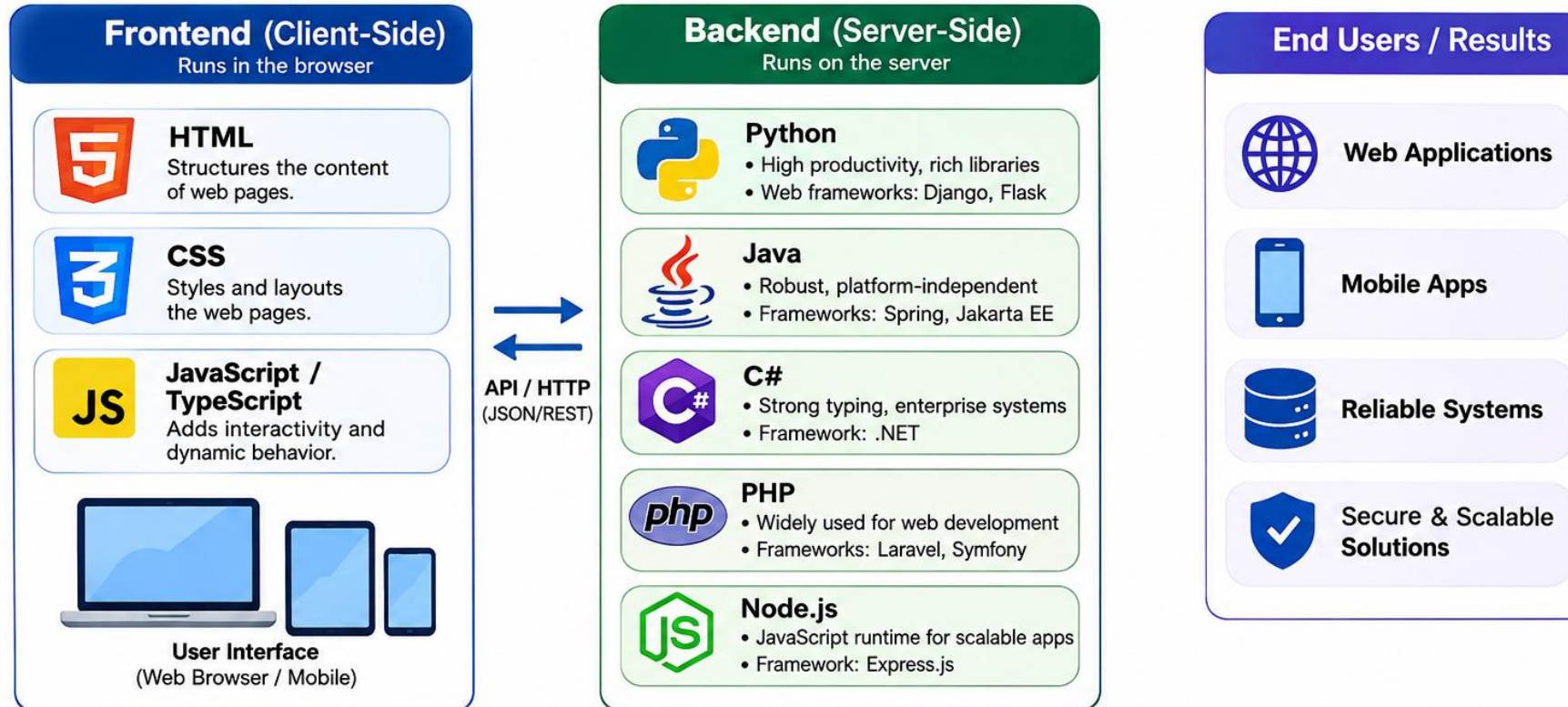
# Evolution of Regulatory Databases





# Programming Languages

Build modern, responsive and powerful web applications



**Key Takeaway:** Frontend technologies (HTML, CSS, JavaScript/TypeScript) create the user experience, while backend technologies (Python, Java, C#, PHP, Node.js, etc.) power the logic, data and business rules.

# Standardised minimum dataset required for an interoperable exchange

7

- Unique Practitioner Identifier
- Personal identifiers
- Professional details
- Registration information
- Licensing information
- Professional standing
- Verification information
- Contact information



# CORE DATABASE COMPONENTS



## 1 MASTER TABLES



Store core, authoritative data about main entities in the system.

### Examples

- Customers
- Employees
- Products
- Accounts

## 2 TRANSACTION TABLES

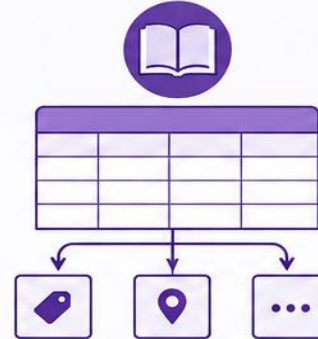


Store records of business events and activities that occur in the system.

### Examples

- Orders
- Payments
- Invoices
- Shipments

## 3 REFERENCE TABLES



Store standardized values used for lookups and to maintain data consistency.

### Examples

- Countries
- Currencies
- Status Codes
- Categories

## 4 AUDIT LOGS



Track changes and activities to support security, compliance and troubleshooting.

### Examples

- User Logins
- Data Changes
- Record Updates
- Deletions

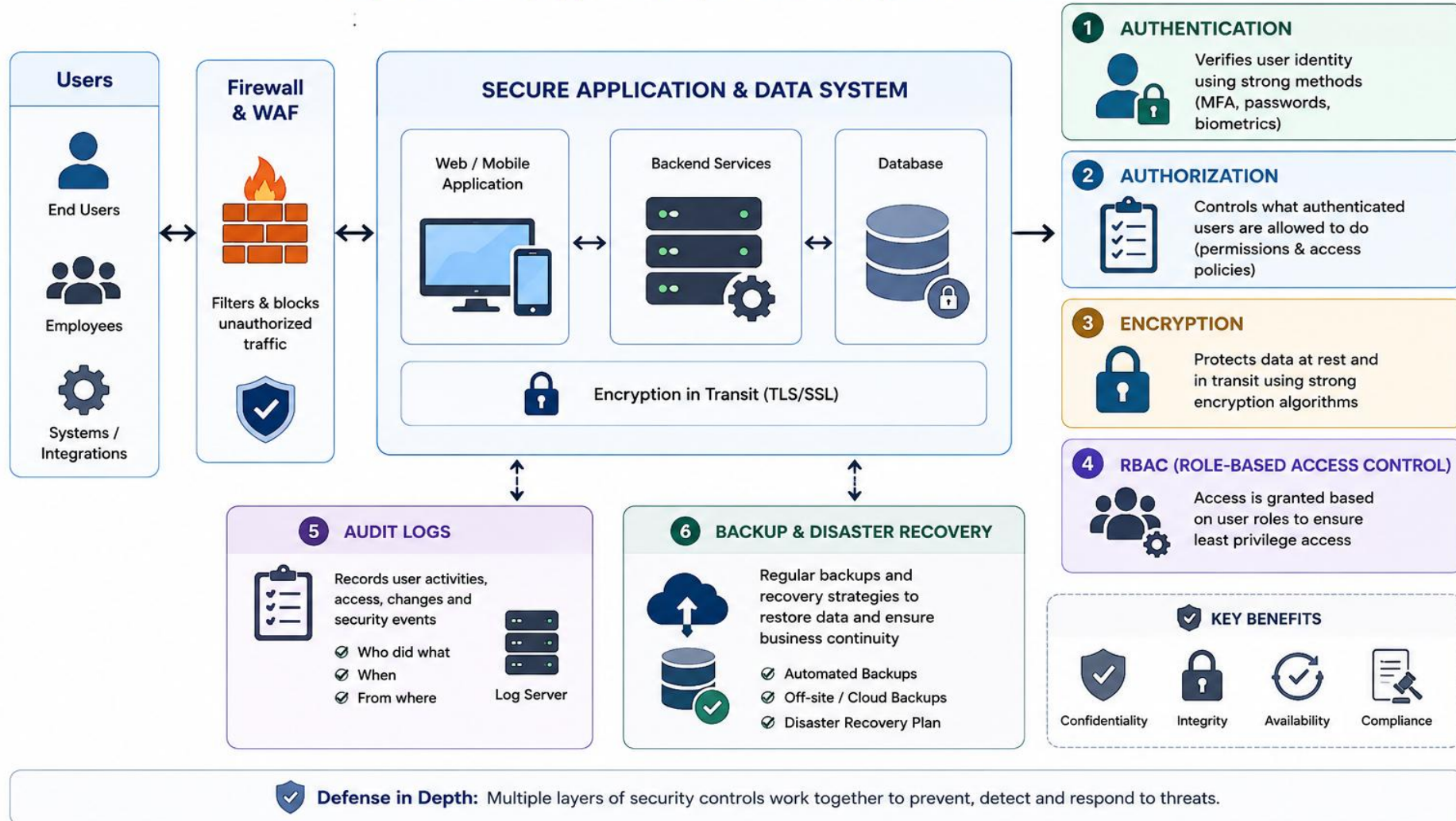






# SECURITY ARCHITECTURE

Layered security approach to protect data, systems and users



# AVAILABLE OPPORTUNITIES IN TECHNOLOGY

10

## Cloud Architecture

- Elastic scaling
- Managed backups
- Disaster recovery
- Data sovereignty considerations

## AI in Regulatory Databases

- Fraud detection
- Duplicate detection
- Predictive licensing
- Compliance analytics

# Migration from MCTIS to HPRS-Tanzania Examples

11

- To align with Government e-Government standards.
- To mitigate limitations associated with architecture, scalability, functionality and the ability to accommodate emerging regulatory requirements.

## Major Challenges Experienced During MCTIS → HPRS Migration

| Major Challenge                                   | Key Issues Experienced                                                                                                                  | Possible Causes                                                                                                                                                                        |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Migration &amp; Data Quality</b>          | Incomplete, duplicated or inconsistent practitioner information;                                                                        | inadequate quality legacy data; differences in database structures; inadequate data mapping; lack of standardized data fields and unique practitioner identifiers                      |
| <b>Business Process &amp; Workflow Transition</b> | Existing MCTIS processes did not always translate directly into HPRS; difficulties with new workflows, roles, approvals and permissions | Differences in business rules and system architecture; insufficient documentation of existing processes; evolving regulatory requirements; inadequate process mapping before migration |



# Major Challenges...

12

| Major Challenge                                            | Key Issues Experienced                                                                                                                         | Possible Causes                                                                                                                                             |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System Performance, Integration &amp; Functionality</b> | Login/session issues; payment and control-number challenges; system errors; functionality gaps; difficulties integrating with external systems | Software bugs; incomplete testing; integration/API challenges; infrastructure limitations; changing system requirements                                     |
| <b>People, Change Management &amp; User Adoption</b>       | Learning curve; user resistance; different levels of digital competency; increased demand for technical support and clarification              | Limited training; inadequate change-management preparation; unfamiliarity with new workflows; insufficient user support and communication during transition |

# SPECIFIC ISSUES TO ADDRESS

13

## Governance Principles for Cross-Border Regulatory Data Sharing

- First, cross-border data sharing should be grounded in the rule of law and legal certainty eg: In country authorisation should be secured.
- Second, the governance framework should provide strong privacy and human-rights protection.
- Transparency and accountability are equally important
- There should also be mechanisms for cross-border enforcement and dispute resolution
- Overall, the literature suggests that effective cross-border regulatory data sharing requires a balance between data accessibility and data protection

# SPECIFIC ISSUES TO ADDRESS

14

## Compliance with National Data Protection Legislation While Collaborating Regionally

- Creation of overarching, binding regional treaties that set a baseline standard for data privacy **eg: MALABO Convention as a standard for all member states.**
- Sovereign nations align their domestic data protection acts with a regional model law cross-border compliance becomes streamlined because the legal thresholds for processing, storage, and subject rights share structural equivalence.

**Cross-border regulatory data sharing should be governed by harmonized legal frameworks that respect national sovereignty while establishing trusted mechanisms for lawful data exchange**



# SPECIFIC ISSUES TO ADDRESS

15

## Safeguards Against Unauthorized Access and Misuse of Practitioner Information

- Protection of practitioner information requires a multi-layered information-security framework based on the principles of confidentiality, integrity, and availability
- Practitioner information should be protected through defence-in-depth, combining legal safeguards, governance controls, encryption, authentication, role-based access, auditability, cybersecurity monitoring, and incident response

# SPECIFIC ISSUES TO ADDRESS

16

## Who Should Own, Manage and Oversee a Continental Regulatory Data Platform

- The literature suggests that a continental regulatory data platform should avoid both complete centralization and complete decentralization
- National regulatory authorities should retain ownership and custodianship of practitioner data

# SPECIFIC ISSUES TO ADDRESS

17

## Who Should Own, Manage and Oversee a Continental Regulatory Data Platform

- National regulatory authorities should retain ownership and custodianship of practitioner data, because health and professional regulatory information remains subject to national laws and sovereignty requirements
- Regional governance should address coordination of standards, interoperability, security, and put in place framework for trusted information exchange

# Key Takeaways

18

Effective database architecture should be:

- Secure
- Scalable
- Interoperable
- Reliable
- AI-ready
- Cloud-enable



# ASANTE SANA

- Questions & Discussion