SUPPLEMENTARY MATERIAL S3

Governance and Legal Frameworks

For Preparedness Intelligence Unit (PIU) Implementation

Implementation Toolkit for African Governments

1. Overview

Establishing a Preparedness Intelligence Unit (PIU) requires explicit legal and governance frameworks that authorize data sharing across institutional boundaries while protecting individual privacy and ensuring accountability. This supplementary material provides ready-to-use templates and checklists to support countries in establishing these foundational frameworks.

The governance foundations serve three critical functions: (1) legal authorization for routine cross-institutional data flows during non-emergency periods; (2) protection of personally identifiable information (PII) through role-based access controls (RBAC); and (3) accountability mechanisms ensuring data is used solely for public health purposes.

IMPORTANT: All governance and legal frameworks must be established BEFORE PIU operations commence. Attempting to establish governance retroactively creates legal risk and undermines public trust.

2. Inter-Ministerial Memorandum of Understanding (MOU)

2.1 Purpose of the MOU

The inter-ministerial Memorandum of Understanding (MOU) establishes the legal framework authorizing routine data sharing between health surveillance systems, laboratory networks, meteorological services, and civil registration authorities. This MOU must be signed BEFORE PIU operations commence to ensure all data flows are legally authorized.

2.2 Template MOU Structure

Table 1 provides a complete template for the inter-ministerial data-sharing MOU, specifying all required elements. Countries should adapt this template to align with national legal frameworks and institutional structures.

Table 1. Inter-Ministerial MOU Template for PIU Data Sharing

MOU Element	Required Content
1. Parties	Ministry of Health (lead agency), National Meteorological Service, Ministry of Agriculture, Civil Registration Authority, National Laboratory System, [other relevant agencies]
2. Purpose	Establish legal framework for routine sharing of surveillance, laboratory, climate, and mortality data to support continuous public health emergency preparedness intelligence
3. Data Ownership	Each agency retains ownership of data originating from its systems. PHEOC/PIU serves as authorized user, not data controller.
4. Data Categories	Specify exactly which data elements will be shared: • Health: electronic Integrated Disease Surveillance and Response (eIDSR) case-level data, aggregate disease counts, outbreak alerts • Laboratory: Test results, pathogen typing, antimicrobial resistance patterns • Climate: Rainfall, temperature, flood

https://doi.org/10.37432/jieph-d-25-00266

MOU Element	Required Content
	alerts, drought indices • Mortality: Weekly death counts by district, cause-of-death patterns
5. Access Permissions	Define who can access what: • PIU Epidemiologist: case-level health data, aggregated lab/climate • PIU Data Scientist: aggregated data only across all sources • PIU Operations Planner: resource allocation data, logistics • PIU Communications Officer: anonymized summaries only
6. Data Protection	Reference national data protection legislation. Specify: • Encryption requirements (data in transit and at rest) • De-identification protocols for research/publication • Breach notification procedures within 72 hours • Annual Data Protection Impact Assessments (DPIAs)
7. Retention Periods	• Real-time operational data: retained 24 months in PIU systems • Historical trends: retained 10 years in anonymized form • Individual identifiers: purged after contact tracing completed • Deletion requests honored within 30 days
8. Data Sharing Frequency	• eIDSR surveillance: real-time automated feed (within 24 hours of entry) • Laboratory confirmations: within 24 hours of result • Climate data: daily automated feed • Mortality data: weekly aggregated reports
9. Technical Standards	• Data formats: District Health Information Software 2 (DHIS2) Application Programming Interface (API), Health Level 7 Fast Healthcare Interoperability Resources (HL7 FHIR) for lab data, CSV for climate • Interoperability: RESTful APIs with Open Authorization 2.0 (OAuth 2.0) authentication • Uptime: 99% service availability target
10. Governance Structure	Establish Data Governance Committee meeting quarterly: • Chair: Director General of Health or designee • Members: Agency heads or senior technical representatives • Mandate: resolve data quality issues, approve new data streams, review compliance
11. Costs	Each agency bears costs of data preparation/sharing from existing budgets. PHEOC covers integration costs. No financial transfers between agencies.
12. Duration and Review	• Initial term: 5 years with automatic renewal • Annual review by Data Governance Committee • Amendment by mutual written consent • 90-day termination notice required
13. Signatures	Minister of Health, Director of Meteorological Service, Director General Civil Registration, National Laboratory Director, [others]

2.3 Process for MOU Negotiation and Signature

Phase 1: Pre-Negotiation (Weeks 1–4)

- Ministry of Health (as lead agency) convenes initial stakeholder meeting with all agencies that will be party to the MOU
- Present PIU concept, operational requirements, and proposed data flows
- Identify agency-specific concerns regarding data sovereignty, technical capacity, and costs
- Establish technical working group with legal and Information Technology (IT) representatives from each agency

Phase 2: Draft Development (Weeks 5–8)

- Technical working group drafts MOU using template (Table 1) as foundation
- Legal counsel from each agency reviews draft for compliance with national data protection legislation
- Specify exact data elements to be shared (attach data dictionaries as annexes)

https://doi.org/10.37432/jieph-d-25-00266

- Define technical protocols and interoperability standards

Phase 3: Internal Approvals (Weeks 9–12)

- Each agency submits draft MOU through internal approval processes
- Address concerns raised during internal reviews through technical working group
- Finalize MOU text with all amendments incorporated

Phase 4: Signature and Activation (Weeks 13–16)

- Schedule signature ceremony with ministers/agency heads
- Establish Data Governance Committee with first meeting scheduled within 30 days
- Activate technical data-sharing infrastructure within 60 days of signature
- Publicize MOU (executive summary only, protecting sensitive technical details)

3. National Legislation for Public Health Data Sharing

3.1 Legislative Requirements

Many countries will require national legislation or ministerial regulations explicitly authorizing real-time data sharing for public health emergency preparedness. The MOU alone may be insufficient without this higher legal authority.

3.2 Option 1: Amendment to Existing Public Health Act

If your country has existing public health emergency legislation, introduce an amendment adding a new section:

SAMPLE LEGISLATIVE LANGUAGE — Section X: Data Integration for Emergency Preparedness

(1) The Minister of Health is hereby authorized to establish integrated surveillance systems combining data from health facilities, laboratories, meteorological services, and civil registration authorities for purposes of detecting, forecasting, and responding to public health emergencies.

(2) All government agencies holding data relevant to public health emergency preparedness shall, upon request of the Minister of Health, share specified data with the designated Public Health Emergency Operations Centre (PHEOC) under terms established in an inter-ministerial Memorandum of Understanding (MOU) and subject to data protection safeguards prescribed herein.

3.3 Option 2: Ministerial Regulation

Where parliamentary processes are slow, a ministerial regulation under existing public health acts may provide interim authority. Consult your legal department on the appropriate regulatory pathway.

4. Role-Based Access Control (RBAC) Matrix

Table 2 defines the data access permissions for each PIU role. This matrix must be technically implemented in DHIS2 and all connected systems before PIU operations commence.

Table 2. PIU Role-Based Access Control (RBAC) Matrix

Data Category	PIU Lead (Epidemiologist)	Data Scientist	Operations Planner	Communications Officer	External Partners
Case-level eIDSR data (PII)	READ	No access	No access	No access	No access
Aggregated disease counts	READ	READ	READ	READ	READ (approved)
Laboratory results (identifiable)	READ	No access	No access	No access	No access

https://doi.org/10.37432/jieph-d-25-00266

Data Category	PIU Lead (Epidemiologist)	Data Scientist	Operations Planner	Communications Officer	External Partners
Laboratory results (aggregated)	READ	READ	READ	READ	READ (approved)
Climate/environmental data	READ/WRITE	READ/WRITE	READ	READ	No access
Resource/logistics data	READ	READ	READ/WRITE	No access	No access
Dashboard analytics	READ/WRITE	READ/WRITE	READ	READ	READ (approved)
Public communications drafts	READ	No access	READ	READ/WRITE	No access

Note: READ = view data only; WRITE = enter or modify data; PII = personally identifiable information. Access permissions are implemented technically through database user roles and enforced through system architecture. Annual review of all access permissions is required, with immediate revocation upon staff departure.

5. Data Protection Compliance Checklist

5.1 Alignment with National Data Protection Legislation

Most African countries have enacted or are enacting data protection legislation aligned with international standards (African Union (AU) Convention on Cyber Security and Personal Data Protection; EU General Data Protection Regulation (GDPR) principles). The PIU must comply fully with applicable national legislation.

5.2 Compliance Checklist

Use this checklist to verify compliance before PIU operations commence:

Legal Basis for Processing

☐ MOU signed by all data-sharing agencies
☐ National legislation or ministerial regulation authorizing data sharing
☐ Public health emergency exemption documented in compliance files

Data Minimization

☐ Only essential data elements are collected/shared (data dictionaries approved)
☐ PII restricted to epidemiologist role only through access controls
☐ Aggregation performed at lowest level that maintains analytical utility

Purpose Limitation

☐ Data use restricted to public health emergency preparedness/response
☐ Staff signed confidentiality agreements prohibiting unauthorized disclosure
☐ Audit logs track all data access with justification required for PII queries

Security Safeguards

☐ Data encrypted in transit (Transport Layer Security (TLS) 1.3 or higher) and at rest (Advanced Encryption Standard 256-bit (AES-256))
☐ Multi-factor authentication required for all PIU system access
☐ Annual penetration testing and vulnerability assessments
☐ Incident response plan with 72-hour breach notification protocol

https://doi.org/10.37432/jieph-d-25-00266

Retention Limits

☐ PII purged within 30 days after contact tracing completed
☐ Operational data retained maximum 24 months
☐ Historical trends anonymized and retained 10 years for research
☐ Automated deletion scripts implemented and tested

Individual Rights

☐ Process for individuals to request access to their data
☐ Correction mechanism for inaccurate data within 30 days
☐ Deletion requests honored except when retention required by law
☐ Public-facing privacy notice explaining PIU data practices

Accountability

☐ Data Protection Impact Assessment (DPIA) completed and approved
☐ Data Protection Officer designated (or equivalent)
☐ Annual compliance audits scheduled
☐ Breach register maintained with corrective actions documented

6. Data Governance Committee: Terms of Reference

6.1 Purpose

The Data Governance Committee provides ongoing oversight of PIU data practices, resolves inter-agency disputes, and ensures continuous compliance with legal frameworks. It reports to the Director General of Health and serves as the highest oversight body for PIU data governance.

6.2 Composition

- Chair: Director General of Health (or designee at Director level)
- Members: Senior technical representatives from each agency party to the MOU (equivalent to Director or Deputy Director level)
- Technical Secretary: PIU Lead (non-voting; provides secretariat support)
- Legal Advisor: Ministry of Health Legal Counsel (non-voting; advisory)
- Data Protection Advisor: National Data Protection Authority representative (if such authority exists)

6.3 Mandate

- Review PIU performance quarterly (based on metrics in Supplementary Material S6)
- Approve additions of new data sources or changes to data-sharing protocols
- Resolve data quality issues or inter-agency disputes within 30 days
- Ensure compliance with MOU terms and national data protection legislation
- Review and approve annual DPIAs
- Recommend amendments to MOU or legal frameworks as needed

6.4 Meeting Schedule

- Quarterly meetings (minimum 4 per year) scheduled in advance
- Extraordinary meetings convened by Chair within 14 days if urgent issues arise
- Quorum: Chair plus representatives from at least 3 agencies
- Decisions by consensus; if consensus not achieved, Chair has tie-breaking vote

https://doi.org/10.37432/jieph-d-25-00266

6.5 Reporting

- Minutes circulated to all members within 14 days of meeting
- Annual report to Minister of Health summarizing PIU performance, data governance issues, and recommendations
- Annual public-facing summary (protecting sensitive details) published on Ministry website

7. Breach Notification and Incident Response Protocol

7.1 Definition of Data Breach

A data breach is any unauthorized access to, disclosure of, loss of, or alteration to personally identifiable health data. This includes unauthorized access to case-level surveillance data, accidental email of PII to unintended recipients, theft or loss of devices containing unencrypted PII, hacking or malware compromising PIU systems, and insider misuse of data for non-public-health purposes.

7.2 Immediate Response (0–24 Hours)

- Any PIU staff discovering potential breach must immediately notify PIU Lead
- PIU Lead notifies PHEOC Director and Data Protection Officer within 2 hours
- Contain breach: disable compromised accounts, isolate affected systems, preserve evidence
- Preliminary assessment: number of individuals affected, sensitivity of data, likelihood of harm

7.3 Investigation and Notification (24–72 Hours)

- Full forensic investigation to determine scope and root cause
- If breach affects >10 individuals OR involves highly sensitive data (e.g., HIV status): notify National Data Protection Authority within 72 hours; notify affected individuals within 72 hours (through District Health Officers if contact tracing data); notify Data Governance Committee Chair within 72 hours
- Public notification required if breach poses high risk to rights/freedoms (Committee decision)

7.4 Remediation and Prevention (Weeks 1–4)

- Implement corrective actions to prevent recurrence
- Document breach in Breach Register with timeline, affected individuals, and corrective actions
- Report to Data Governance Committee at next quarterly meeting
- Update staff training to address root causes

8. Implementation Checklist for Governments

Use this master checklist to track progress on governance establishment before PIU operations commence.

Phase 1: Legal Foundation (Months 1–4)

☐ Convene inter-ministerial stakeholder meeting
☐ Establish technical working group for MOU drafting
☐ Draft MOU using template (Table 1)
☐ Identify need for legislation versus regulation
☐ Draft legislative amendment or regulation (if required)
☐ Submit legislation/regulation for approval

Phase 2: MOU Finalization (Months 3–4)

☐ Legal review by all agencies completed

https://doi.org/10.37432/jieph-d-25-00266

☐ Internal approvals obtained from each agency
☐ MOU signature ceremony scheduled
☐ MOU signed by all parties
☐ Executive summary publicized

Phase 3: Operational Frameworks (Months 4–5)

☐ Data Governance Committee established
☐ Terms of Reference approved
☐ First Committee meeting held
☐ Meeting schedule for year established
☐ Role-based access control (RBAC) matrix approved (Table 2)
☐ Access controls implemented in IT systems

Phase 4: Compliance (Months 5–6)

☐ Data Protection Impact Assessment (DPIA) completed
☐ Compliance checklist verified (all items checked)
☐ Breach notification protocol adopted
☐ Staff confidentiality agreements signed
☐ Privacy notice published on website
☐ Data Protection Officer designated

Ready for Operations

☐ All above items completed and documented
☐ Attorney General certification of legal compliance
☐ Approval from Data Governance Committee to commence PIU operations

Do not commence PIU operations until all governance items above are complete. This checklist should be reviewed and certified by the PHEOC Director before data flows are activated.

9. Conclusion

Robust governance and legal frameworks are non-negotiable prerequisites for PIU operations. These frameworks protect individual privacy, ensure data is used solely for public health purposes, and create accountability mechanisms that build public trust.

Countries should complete all elements of the implementation checklist BEFORE recruiting PIU staff or activating data flows. Attempting to establish governance retroactively after operations have commenced creates legal risk and undermines public confidence.

The templates and tools in this supplementary material are designed to be adapted to national contexts while maintaining international best practices for data protection and public health surveillance. For staffing and SOPs, see Supplementary Material S1. For the implementation timeline for governance establishment, see Supplementary Material S2.

https://doi.org/10.37432/jieph-d-25-00266

List of Abbreviations

Abbreviation	Full Term
AES-256	Advanced Encryption Standard 256-bit
Africa CDC	Africa Centres for Disease Control and Prevention
API	Application Programming Interface
AU	African Union
DHIS2	District Health Information Software 2
DPIA	Data Protection Impact Assessment
eIDSR	Electronic Integrated Disease Surveillance and Response
EU	European Union
FETP	Field Epidemiology Training Programme
GDPR	General Data Protection Regulation (EU)
HL7 FHIR	Health Level 7 Fast Healthcare Interoperability Resources
IT	Information Technology
MOU	Memorandum of Understanding
OAuth 2.0	Open Authorization 2.0 (authentication standard)
PHEOC	Public Health Emergency Operations Centre
PIU	Preparedness Intelligence Unit
PII	Personally Identifiable Information
RBAC	Role-Based Access Control
TLS	Transport Layer Security
USD	United States Dollars
WHO	World Health Organization

https://doi.org/10.37432/jieph-d-25-00266