Strengthening Global Governance for AI-Enabled Biological Threat Detection

Sandra Matinyi , Gerald Mboowa, Bryan Tegomoh

sandramatinyi@gmail.com , gmboowa@gmail.com, bryan.tegomoh@gmail.com

Abstract

Artificial intelligence (AI) is rapidly transforming biological surveillance and public health preparedness by enabling faster detection of emerging pathogens, unusual transmission patterns, and potential biological threats. However, the growing integration of AI into biological threat detection introduces major governance challenges related to data sharing, model transparency, dual-use risks, accountability, and unequal global access to AI infrastructure. Existing global governance frameworks remain fragmented and ill-equipped for AI-era biological detection systems. This paper examines how governance frameworks can be strengthened to ensure that AI-enabled biological threat detection systems are effective, equitable, secure, and resistant to misuse. Drawing on a systematic review of 34 sources and a catalogue of 23 AI-enabled tools, we propose and apply a seven-dimension Governance Readiness Framework, STAE+ framework, to evaluate two representative systems - WHO EIOS and SeqScreen. Both tools score in the moderate range when assessed by raw score (EIOS 54/102; SeqScreen 55/102), but are reclassified as Low Governance Readiness under the Framework's Override Clause, which is triggered by critical zero scores on Accountability sub-dimensions in both tools, and additionally on Incident Reporting for SeqScreen. We argue that governance mechanisms must be grounded in transparency, accountability, equity, and shared security, and propose a structured set of recommendations with designated actors. Africa is used as the primary LMIC lens throughout, as the region carrying the highest relevant disease burden relative to AI tool development capacity.

1. Introduction

Artificial intelligence is transforming biological surveillance at a pace that governance systems have not matched. Biosurveillance platforms now integrate genomic, epidemiological, environmental, and mobility data to identify biological threats with unprecedented speed, while protein design tools such as AlphaFold 3, RFDiffusion, and ProteinMPNN can generate novel biological structures at scale, simultaneously advancing beneficial science and biosecurity risk (Wittmann et al., 2025; Ahdritz et al., 2024). The governance frameworks intended to regulate biological threats, the WHO International Health Regulations, the Biological Weapons Convention, and the 2025 WHO Pandemic Agreement were designed before advanced AI existed as a regulatory concern. They address biological agents and disease reporting, but not algorithmic oversight, AI-generated sequences, or cross-border data flows from automated surveillance systems (Parums, 2025; Pannu et al., 2025). Critical questions of accountability, transparency, data ownership, dual-use risk, and equitable access remain unresolved, with particular consequence for low- and middle-income countries that risk becoming dependent on externally controlled AI infrastructures they did not design and cannot govern (Munung et al., 2024; NTI, 2024). This paper addresses that gap empirically through a systematic inventory of 23 AI-enabled tools, a structured stakeholder mapping, and a governance readiness evaluation applied to two case study tools and proposes governance reforms grounded in transparency, accountability, equity, and shared security.

2. Background

AI-enabled biological threat detection refers to the use of machine learning, natural language processing, and predictive analytics to identify, monitor, and forecast biological risks using genomic sequences, clinical records, epidemiological reports, environmental signals, and mobility data (WHO, 2021). A central concern is dual-use risk, the same AI systems that accelerate pathogen detection may also facilitate harmful biological research or lower barriers to dangerous biological knowledge generation (Pannu et al., 2025). This challenge is compounded by the convergence of AI with synthetic biology, where generative design tools capable of producing novel protein sequences are now publicly accessible without binding governance frameworks governing their biosecurity implications (Wittmann et al., 2025; FAS, 2024). This paper builds on scholarship in AI ethics, biosecurity governance, and global health equity particularly work on transparency, accountability, responsible

innovation, equitable data governance, and data sovereignty, which argues that countries contributing biological data should retain meaningful authority over how those data are stored, analysed, shared, and commercialised (NTI, 2024; Thaldar, 2024; Munung et al., 2024). Rather than opposing technological advancement, the analysis argues for governance architectures that enable innovation while reducing catastrophic risks, preventing exploitative practices and promoting equitable participation in global biosecurity systems.

3. Methodology

This study employs three integrated components, a systematic literature review for tool identification, a purposive stakeholder mapping exercise, and a structured governance readiness framework evaluation applied to selected case study tools. Africa was selected as the primary regional LMIC focus.

3.1 Literature review and tool identification

AI-enabled biological threat detection tools were identified through systematic review of 34 source documents compiled between 2022 and 2026, spanning peer-reviewed literature, institutional grey literature, policy analyses, and technical documentation from WHO, ECDC, IBBIS, NTI, CSIS, CSET, and academic institutions including UNSW, Rice University, and the University of Washington. Tool inclusion required sufficient published information to characterise developer identity, AI methodology, access model, and operational status. Tools were organised into four functional categories: biosurveillance platforms (A), epidemic early warning systems (B), nucleic acid sequence screening tools (C), and dual-use AI protein design tools (D). The resulting catalogue of 23 tools reflects what is visible within this bounded, predominantly anglophone literature set. Tools developed or deployed primarily within LMIC contexts are underrepresented, a limitation that is directly relevant to the equity dimension of the governance analysis.

3.2 Stakeholder mapping methodology

Stakeholder identification followed a purposive, iterative approach guided by the research question: who governs, develops, deploys, or is affected by AI-enabled biological threat detection systems? Three strategies were applied sequentially. First, institution-level actors were identified directly from the 34-source literature set, any institution named as a developer, standard-setter, funder, or governance body was included. Second, a governance landscape scan using WHO, Africa CDC, BWC intersessional, and IBBIS grey literature identified regulatory and normative actors not visible in tool-specific literature. Third, affected community actors were identified through health data governance literature, recognising that communities whose biological data underpin AI biosurveillance systems are rarely named in technical literature but represent fundamental governance stakeholders.

Actors were categorised into six tiers, multilateral and intergovernmental organisations, African regional institutions, national public health institutes, academic and research networks, private sector technology developers, and civil society and affected communities. Each actor was assessed across four dimensions: role in AI biosurveillance governance, key tools or programmes, governance capacity, and primary governance concern. Table S1 presents 16 key actors drawn from a broader mapping of 29 actors conducted during the study.

3.3 Regional focus: Africa as LMIC Representative

Africa was selected as the primary LMIC regional focus for three reasons. First, Africa carries the highest burden of the infectious diseases most relevant to AI biosurveillance including Ebola, Lassa fever, Marburg, and emerging epidemic-prone pathogens yet generates a disproportionately small share of the AI biosurveillance tools designed to detect them. This asymmetry between burden and technical capacity makes Africa the sharp lens through which to examine the equity dimension of AI biosurveillance governance.

Second, Africa has developed a notable regional institutional architecture for health data governance, including the AU Data Policy Framework (2022), the AU Continental AI Strategy (2024–2030), and the Africa CDC Flagship Initiative on Health Data Governance, launched in 2023. These instruments provide an existing policy baseline against which governance gaps can be identified, making the analysis more grounded. Whether this architecture

is more developed than equivalent regional frameworks in Latin America or Asia is beyond the scope of this study, the argument is that it is sufficiently developed to make governance gap analysis tractable and specific.

Third, the actor mapping conducted provided a structured starting point for stakeholder identification, covering Africa CDC, AUDA-NEPAD, NICD, ACEGID, KEMRI-Wellcome, Institut Pasteur Dakar, SACIDS, H3ABioNet, and AIMS. Each actor's role, deployment status, and governance position was subsequently validated against current institutional documentation and peer-reviewed literature.

Africa's experience is taken as illustrative of broader LMIC dynamics rather than exhaustive of them. The governance gaps identified, data sovereignty deficits, structural technology dependence, exclusion of affected communities, and underrepresentation of LMIC institutions as co-developers apply with varying severity across South Asia, Southeast Asia, and Latin America.

3.4 STAE+ Governance Readiness Framework Development

The Governance Readiness Framework (GRF) was developed through synthesis of existing governance frameworks in AI ethics (WHO, 2021), biosecurity (NASEM, 2025; NTI, 2024), and global health equity (OECD, 2025; Munung et al., 2024). It operationalises seven governance dimensions, Safety, Transparency, Accountability, Equity, Data Governance, Dual-Use Risk, and Sustainability into 34 scored sub-dimensions. Two tools were selected for the framework application: WHO EIOS and SeqScreen, chosen because they span opposite ends of the institutional spectrum, allowing the framework to be stress-tested against contrasting governance arrangements. Scores are based on published evidence only.

4. AI Tool Landscape

The systematic review identified 23 AI-enabled tools across four functional categories. The distribution reveals significant geographic concentration: all 23 tools are developed in North America, Western Europe, or Australia. Africa and other LMIC appear almost exclusively as deployment contexts, not as developer actors. The catalogue also reveals a structural asymmetry: dual-use AI protein design tools (Category D) are fully open-source with no binding oversight, while the sequence screening tools designed to detect their outputs operate under voluntary standards only.

Table 2: AI-Enabled Biological Threat Detection - Tool catalogue (23 Tools)

#	Tool	Category	Developer/HQ	AI Technology	Access	Deployment	Citation
A1	**BlueDot Insights**	Biosurveillance	BlueDot Inc., Canada	NLP, ML, LLM, FME	Commercial	Operational - global	(MacIntyre et al., 2023)
A2	**HealthMap**	Biosurveillance	Harvard/Boston Children's Hospital, USA	NLP, text classification	Free/Open	Operational - global	(Brownstein et al., 2008)
A3	**EIOS**	Biosurveillance	WHO/EC JRC, Switzerland	AI aggregation, NLP	Restricted (govts)	Operational - 110+ countries (WHO 2026)	(WHO, 2024a; WHO, 2026)
A4	**GPHIN**	Biosurveillance	Public Health Agency Canada	NLP, multilingual	Subscription	Operational - global, WHO feed.	(MacIntyre et al., 2023)
A5	**GBSP**	Biosurveillance	U.S. DoD, USA	AI predictive analytics	Govt restricted	Operational - US govt only	(MacIntyre et al., 2023)
A6	**Metabiota**	Biosurveillance	Metabiota/Airfinity/Munich Re	Big data, cloud ML	Commercial	Operational - commercial	(MacIntyre et al., 2023)
B1	**EPIWATCH**	Early Warning	UNSW/Kirby Inst., Australia	NLP, NER, GIS	Free (public)	Operational - global incl. Africa	(MacIntyre et al., 2023)
B2	**ProMED-mail**	Early Warning	ISID, USA	Human moderation	Free/Open	Operational - 150+ countries	(Carrion & Madoff, 2017)
B3	**Epitweetr**	Early Warning	ECDC, Sweden	R-based, social NLP	Free/Open-source	Operational - ECDC member states	(MacIntyre et al., 2023)
B4	**Google Flu Trends**	Early Warning	Google, USA	Search query ML	Discontinued	Discontinued (2015)	(MacIntyre et al., 2023)
B5–7	**FLUCAST/EPIRISK/ORIGINS**	Early Warning	UNSW/EPIWATCH suite	AI forecasting sub-tools	Via EPIWATCH	Operational - via EPIWATCH	(MacIntyre et al., 2023)
C1	**commec**	Sequence Screening	IBBIS/NTI, Switzerland	HMM, BLASTX/N, DIAMOND	Free/Open-source	Operational - global (2024)	(Wheeler et al., 2024; IBBIS, 2024)
C2	**Aclid**	Sequence Screening	Aclid, USA	Seq DB, hw-accel alignment	Commercial	Operational - synthesis providers	(Wittmann et al., 2025)
C3	**FAST-NA Scanner**	Sequence Screening	BBN/Raytheon, USA	Seq analysis pipeline	Govt/Commercial	Operational	(Wittmann et al., 2025)

#	Tool	Category	Developer/HQ	AI Technology	Access	Deployment	Citation
C4	**UltraSeq**	Sequence Screening	Battelle, USA	Alignment-based screening	Govt/Commercial	Operational	(Wittmann et al., 2025)
C5	**SecureDNA**	Sequence Screening	SecureDNA Consortium	Cryptographic + ML	Free/Open	Operational - 2024	(IBBIS, 2024)
C6	**SeqScreen**	Sequence Screening	Rice Univ./Signature Science, USA	ML functional screening	Academic/Open	Research / Emerging	(Balaji et al., 2022)
D1	**AlphaFold 3**	AI Protein Design (Dual-Use)	Google DeepMind, UK	Deep learning, diffusion	Open (restricted)	Operational - Dual use risk	(Wittmann et al., 2025)
D2	**RFDiffusion/ProteinMPNN**	AI Protein Design (Dual-Use)	Baker Lab, UWash., USA	Diffusion + inv. folding	Open-source	Operational - Dual use risk	(Wittmann et al., 2025; FAS, 2024)
D3	**LigandMPNN**	AI Protein Design (Dual-Use)	Baker Lab, UWash., USA	Neural net seq. design	Open-source	Operational - Dual use risk	(Wittmann et al., 2025)
D4	**OpenFold**	AI Protein Design (Dual-Use)	Academic Consortium, USA	AlphaFold2 retrain, fully open	Open-source	Operational - Dual use risk	(Ahdritz et al., 2024; Wittmann et al., 2025)

5. Stakeholder Mapping

Understanding the governance landscape requires identifying who the key actors are, what interests they bring, and where their governance authority begins and ends. Table S1 presents 16 key stakeholders across six tiers. Africa-focused institutions are shaded green.

Table S1: Key Stakeholders - AI-Enabled Biological Threat Detection Governance

Green shading = Africa-based or Africa-focused institutions.

Actor	Tier	HQ	Role in AI Biological threat detection Governance	Key Tool / Programme	Primary Governance Concern
Global — Multilateral & Intergovernmental					
WHO	Global	Geneva	Sets global norms; operates EIOS; administers IHR (2005, amended 2024) and 2025 Pandemic Agreement	EIOS; IHR; WHO Pandemic Agreement (2025)	WHO operates EIOS
BWC State Parties	Global	183 states	Prohibits biological weapons; intersessional process discusses dual-use research of concern	BWC Review Conferences; intersessional process	No verification mechanism
IBBIS	Global	Geneva	Technical standard-setter for DNA synthesis screening; coordinates AI red-teaming; bridges science and governance	commec; ISO 20688-2:2024; IGSC Harmonized Protocol	Voluntary standards only; no binding mandate
Africa — Regional Institutions					
Africa CDC	Regional	Addis Ababa	Continental coordinator for pathogen genomics and health security; leads Biosafety & Biosecurity Strategy 2025–2030 and health data governance Flagship Initiative	Africa PGI; Health Data Governance Initiative; BBI 2025–2030	All AI technology partners are external. No Africa-developed AI biosurveillance tool exists. Structural technology dependence remains the primary challenge (Africa CDC, 2025)
WHO AFRO	Regional	Brazzaville	Deploys EIOS across 47 African member states; coordinates IHR implementation; mediates between WHO Geneva and African NPHIs	EIOS (47 AFRO states); IHR focal point network	Signal-to-action gap: early alerts reach governments that lack outbreak response capacity. Warning without response does not reduce mortality (MacIntyre et al., 2023)
H3ABioNet	Regional	Cape Town + 30 nodes	Pan-African bioinformatics backbone; builds AI genomic analysis capacity across 30+ institutions; addresses bioinformatician shortage	Pan-African bioinformatics pipelines; genomic analysis tools	Addresses Africa's largest AI biosurveillance constraint human capacity but cannot substitute for national NPHI investment in AI tool deployment (Munung et al., 2024)
Africa — National Public Health Institutes					

Actor	Tier	HQ	Role in AI Biological threat detection Governance	Key Tool / Programme	Primary Governance Concern
NICD (South Africa)	National	Johannesburg	Africa's foremost genomic epidemiology institution; regional SADC reference laboratory; leads AI-assisted AMR and variant surveillance	AI bioinformatics pipelines; Africa PGI; AMR detection	Strongest AI biosurveillance capacity on continent but concentrated in South Africa and not automatically transferable to other AU member states
ACEGID (Nigeria)	National	Ede, Nigeria	West Africa reference centre for pathogen genomics; Lassa fever, Ebola, Mpox surveillance	Africa PGI; AI-assisted sequence analysis	Data contributor to AI biosurveillance without co-governance rights. Genomic data extracted for external AI model training without documented benefit-sharing (Rebai et al., 2025)
KEMRI-Wellcome (Kenya)	National	Kilifi, Kenya	AI-enabled pathogen genomics and malaria surveillance; core East Africa surveillance node; generates data for regional AI platforms	AI pathogen genomics; AMR monitoring; East Africa biosurveillance	Wellcome Trust funding dependency creates sustainability risk. No enforceable data sovereignty protections
Academic & Private Sector — Tool Developers					
UNSW/Kirby Institute	Academic	Sydney, Australia	Developed EPIWATCH — the most documented open-source early warning system with confirmed Sub-Saharan Africa detection	EPIWATCH; FLUCAST; EPIRISK; ORIGINS	Externally developed and managed. African institutions are end-users. No African institution co-develops the platform monitoring African outbreak signals (MacIntyre et al., 2023)
Google DeepMind	Private	London, UK	Developed AlphaFold 3. Voluntary restricted access via AlphaFold Server. No biosecurity governance role	AlphaFold 3	Evaded all tested biosecurity screening tools (Wittmann et al., 2025). No binding framework governs its use in biosecurity-sensitive contexts
Baker Lab (UWash.)	Academic	Seattle, USA	Develops open-source AI protein design tools — the primary technical challenge to biosecurity screening systems	RFDiffusion; ProteinMPNN; LigandMPNN	Open-source with no access controls. No formal biosecurity governance engagement (Wittmann et al., 2025)
NTI	Civil Society	Washington DC	Independent biosecurity policy and advocacy; funded commec development; active Global South AI biosecurity engagement	AIxBio programme; commec co-funder	US-based institution. African institutional co-leadership in AI biosecurity policy remains limited despite NTI's Global South engagement (NTI, 2024)
Affected Communities — Systematically Underrepresented					
African populations & data-contributing communities	Community	Pan-African	Provide biological data underpinning AI biosurveillance systems. Fundamental data rights and benefit-sharing stakeholders	None — data sources, not governance participants	No consent frameworks govern incorporation of community biological data into AI training datasets. No benefit-sharing mechanisms. Zero formal governance authority (Munung et al., 2024; Thaldar, 2024)

Three structural findings emerge from the stakeholder mapping:

First, all 23 AI tools in the catalogue are developed in high-income countries. Africa and the Global South appear exclusively as deployment contexts, not as developers or co-governors of the tools that monitor their populations. This is the most fundamental equity failure in the current landscape.

Second, the actors with the highest formal governance power (WHO, BWC State Parties) have the weakest AI-specific provisions, while the actors with the highest technical capability (Google DeepMind, Baker Lab) operate under voluntary commitments only. This governance capacity inversion is the structural problem that governance reform must address.

Third, affected communities whose biological data underpin AI biosurveillance systems hold no formal governance role in any existing framework. Systems built on data obtained without meaningful consent or benefit-sharing face legitimacy deficits that undermine long-term operational sustainability (Munung et al., 2024; Thaldar, 2024).

6. Governance Analysis

6.1 The Governance Gap

AI-enabled biological threat detection systems are advancing faster than the governance structures designed to regulate them. The global governance architecture for biological threats rests on instruments that were designed for different risk profiles and have not kept pace with AI-enabled biological capabilities. The WHO International Health Regulations (2005, amended 2024) establish disease reporting obligations, PHEIC declaration criteria, and core national surveillance capacity requirements, but contain no provisions governing AI algorithmic operations, transparency requirements for AI-enabled surveillance tools, or data sovereignty protections for AI-generated intelligence.

The WHO Pandemic Agreement, adopted in May 2025, advances pandemic preparedness and pathogen access and benefit-sharing, but its pathogen access and benefit-sharing annex remains unfinished, and the Agreement contains no provisions addressing AI-enabled biosurveillance tools or algorithmic accountability (WHO, 2025; Parums, 2025). The most recent instrument in global health governance therefore confirms rather than closes the gap this study identifies.

The Biological Weapons Convention (1975) establishes the foundational international norm prohibiting the development, production, and stockpiling of biological weapons. Its principles-based architecture was designed to be forward-looking and adaptive rather than prescriptive, allowing it to remain normatively relevant across fifty years of biotechnological change. The more fundamental and enduring problem is the absence of a verification mechanism. The BWC has never had a binding compliance verification system. Six years of multilateral negotiations to establish one collapsed in 2001 when the United States rejected the draft protocol of the Ad Hoc Group, and no comparable effort has since succeeded (Arms Control Association, 2001; Bulletin of the Atomic Scientists, 2024). This means that even where AI-enabled biological tools generate outputs of biosecurity concern, there is no international body with the mandate or investigative capacity to assess whether any state or actor is using such capabilities in violation of the Convention. In practical terms, AI protein design tools such as AlphaFold 3 and RFDiffusion operate in a space the BWC prohibits in principle but cannot verify or enforce in practice, a governance gap that predates AI but that the diffusion of powerful open-source biological AI tools now makes considerably more consequential (Giordano, 2025; Wheeler et al., 2024)

Even in the jurisdictions with the most developed biosecurity screening policy like the USA, the 2024 OSTP Framework was suspended pending replacement in May 2025, illustrating that governance advances remain fragile and reversible even where they exist (Arms Control Association, 2025)

6.2 Data Sovereignty and Equitable Access

Effective biological threat detection depends on international data sharing, but this creates a fundamental tension with data sovereignty. Countries in the Global South, which generate critical biological datasets

frequently have limited influence over how those data are stored, commercialised, or incorporated into proprietary AI infrastructures (NTI, 2024; Munung et al., 2024). Governance frameworks must establish enforceable benefit-sharing arrangements and sovereignty protections as preconditions for data access, not afterthoughts (Rebai et al., 2025).

6.3 Dual-Use Risks and Oversight Limits

The same AI systems that improve pandemic preparedness may lower barriers to dangerous biological experimentation (Pannu et al., 2025). The 2024 Microsoft/IBBIS red-teaming study demonstrated empirically that all four commercially available biosecurity screening systems failed to detect functional protein variants generated by publicly available AI design tools (Wittmann et al., 2025). Open-source availability of RFDiffusion, ProteinMPNN, and OpenFold means the capability to design potentially dangerous sequences is diffusing globally with no binding oversight (Ahdritz et al., 2024).

6.4 Toward a Coordinated Governance Framework

We argue that strengthening governance for AI-enabled biological threat detection requires a coordinated international framework built around four core principles, including Safety, transparency, accountability, equity, and shared security. These are operationalized into seven invaluable dimensions and thirty four subdimensions in Section 7 as the STAE+ Governance Readiness Framework, applied to two tools in Section 8.

7. STAE+ Governance Readiness Framework

The STAE+ provides a structured evaluation tool for assessing whether AI-enabled biological threat detection tools can be responsibly deployed. Seven dimensions with 34 scored sub-dimensions are assessed against published evidence.

7.1 Scoring System

Table 3: Scoring System and Readiness Thresholds

Score	Rating	Meaning	Readiness Threshold
3	Green	Criterion fully met with published evidence	80–100% = High Governance Readiness
2	Yellow	Partially met; some evidence exists but gaps remain	50–79% = Moderate Governance Readiness
1	Blue	Criterion identified but not met; significant gap	<50% = Low Governance Readiness
0	Red	Absent, non-compliant, or not applicable as positive	Override clause — see below

Maximum score: 102 points (34 sub-dimensions × 3). The Override Clause specifies that a score of 0 on any Accountability sub-dimension, or on the Dual-Use Risk - Biological Misuse Potential sub-dimension, automatically triggers a Low Governance Readiness classification regardless of total percentage score. Sub-dimensions marked ★ in Table 4 are override triggers. This clause exists because governance that cannot be enforced, audited, or corrected is not governance. A tool may perform well on transparency and sustainability while being entirely unaccountable; the override prevents that structural failure from being masked by aggregate scoring.

7.2 Framework Dimensions

Table 4: Governance Readiness Framework — 34 Sub-dimensions (★ = Override triggers)

Dimension	Sub-dimension	Key Questions	Score
Safety	Detection accuracy	Is the tool validated against real-world events? Is sensitivity/specificity data published?	0–3

	False positive management	Is a published false-positive rate available? Is human review required before high-consequence action?	0–3
	Human oversight	Is expert review mandatory before action-level outputs? Are named responsible roles documented?	0–3
	Post-deployment monitoring	Are drift detection, incident logging, and update schedules documented?	0–3
	Dual-use / misuse risk	Has a formal biological risk assessment been conducted? Has adversarial testing been performed?	0–3
Transparency	Algorithmic transparency	Is the model methodology or code publicly available? Is training data disclosed?	0–3
	Data source disclosure	Are all input data sources documented? Are known coverage gaps disclosed?	0–3
	Output explainability	Do alerts include source citation, triggering rationale, and confidence scoring?	0–3
	Performance reporting	Is sensitivity/specificity data publicly available, disaggregated by geography and disease type?	0–3
	Language accessibility	Is the tool accessible in languages relevant to its deployment context?	0–3
Accountability ⚠	Developer accountability	Is there a registered legal entity with named governance structure?	0–3
[Override dimension]	Regulatory oversight ★	Is the tool subject to at least one binding governance framework?	0–3
	Incident reporting ★	Is there a mandatory formal protocol for reporting failures to a designated authority?	0–3
	Independent audit	Has a third-party technical review been conducted within the past three years?	0–3
	Redress mechanisms ★	Is there a formal process for affected governments or populations to challenge algorithmic outputs?	0–3
Equity	Access equity	Is access free or subsidised for LMICs? Are infrastructure requirements manageable in low-resource settings?	0–3
	Geographic coverage	Has LMIC coverage been validated? Has a sub-regional bias assessment been published?	0–3
	Data representativeness	Does training/validation data include LMIC populations? Has a demographic bias audit been conducted?	0–3
	Benefit distribution	Is there evidence of positive health impact in LMIC populations — not merely technical accessibility?	0–3
	Governance participation	Do LMIC institutions participate formally in tool governance and development decisions?	0–3
Data Governance	Data ownership	Is it documented who owns data generated, processed, or stored by the tool?	0–3
	Sovereignty protections	Are data sovereignty protections defined and enforceable for data-contributing countries?	0–3
	Cross-border sharing rules	Are cross-border data flows governed by documented consent frameworks?	0–3
	Benefit-sharing	Are benefit-sharing mechanisms documented for countries contributing biological or health data?	0–3
	Consent and re-use	Are clear consent requirements documented? Are limitations on downstream re-use defined?	0–3
Dual-Use Risk	Biological misuse potential ★	Could the tool's outputs facilitate dangerous pathogen engineering?	0–3
	Screening for dangerous outputs	Does the tool actively screen for dangerous sequences or requests?	0–3
	Adversarial testing	Has the tool been formally red-teamed for resistance to deliberate misuse?	0–3

	Access controls	Are access controls documented in proportion to the biological risk level?	0–3
Sustainability	Local operation	Can the tool operate on local infrastructure? Is offline or low-bandwidth operation supported?	0–3
	Local expertise	Is training available in LMIC contexts? Is there a documented capacity-building pathway?	0–3
	Long-term financing	Is there documented long-term institutional financing? Is the tool at risk if a single funder withdraws?	0–3
	Local adaptability	Can LMIC institutions legally and technically modify the tool without requiring developer permission?	0–3
	Technology dependency	Is the tool's continued operation dependent on infrastructure controlled by external entities?	0–3
★ Override triggers		Sub-dimensions marked ★ are Override triggers. A score of 0 on any Accountability sub-dimension, or on Dual-Use Risk — Biological Misuse Potential, automatically classifies the tool as Low Governance Readiness regardless of total percentage score.	

8. Framework Application: Case Studies

The GRF was applied to two tools representing opposite ends of the governance spectrum: EIOS, a multilateral institutional platform with strong intergovernmental accountability structure but limited transparency and no independent regulatory oversight; and SeqScreen, an open-source academic tool with strong technical transparency but operating in a complete regulatory vacuum.

Comparative Governance Readiness Assessment: EIOS vs SeqScreen

Governance Readiness Framework - 34 Sub-dimensions / ★ = Override Clause trigger / Score 0 on any Accountability sub-dimension or Dual-Use Risk - Biological Misuse Potential - Low Governance Readiness regardless of raw score

Score key:

3 = Green — Fully met, published evidence	2 = Yellow — Partially met, gaps remain	1 = Blue — Identified but not met	**0 = Red — Absent / non-compliant ★ = Override trigger**

Sub-dimension	EIOS	EIOS — Key Finding	SeqScreen	SeqScreen — Key Finding
Developer / HQ	WHO / European Commission Joint Research Centre, Geneva		Rice University / Signature Science LLC, USA	
Function	Epidemic intelligence — AI-enabled open-source scanning for outbreak signals; restricted to designated government users		Sequence screening — ML-based functional characterisation of DNA sequences for pathogen and dual-use risk detection; open-source	
SAFETY				
Detection accuracy	**2**	COVID-19 first machine-generated alert 03:14 UTC, 31 Dec 2019; no published Africa-specific sensitivity/specificity data	**2**	Validated in Genome Biology (Balaji et al., 2022); demonstrated COVID-19 sequence detection; no published LMIC-specific validation
False positive management	**2**	AI + expert review chain before WHO escalation; INFORM integration; no published false-positive rate by region	**2**	ML classifiers outperform taxonomy-only approaches; no published false-positive rate for LMIC synthesis orders

Sub-dimension	EIOS	EIOS — Key Finding	SeqScreen	SeqScreen — Key Finding
Human oversight	**3**	WHO expert review mandatory before PHEIC escalation; IHR Art. 12 governs decision-making — strongest oversight of both tools	**2**	Synthesis providers make final decisions; no mandatory training standard for interpreting SeqScreen outputs
Post-deployment monitoring	**2**	EIOS Strategy 2024–2026 includes AI enhancement programme; no independent performance audit published	**1**	Academic maintenance via GitHub; no formal monitoring schedule, drift detection, or incident reporting cadence
Dual-use / misuse risk	**3**	No genetic sequence data processed; access restricted to designated governments; geopolitical misuse risk limited	**1**	Open-source architecture creates adversarial reverse-testing vulnerability: adversaries can test evasion locally before submitting synthesis orders (Wittmann et al., 2025)
TRANSPARENCY				
Algorithmic transparency	**1**	Built on Ozone Widget Framework; AI classification algorithms and alert prioritisation logic not published — black-box system for 120+ governments	**3**	Fully open-source on GitHub (treangenlab/seqscreen); methodology published in Balaji et al. (2022) — complete transparency
Data source disclosure	**2**	Sources documented (ProMED, HealthMap, GPHIN, JHU, Worldometer, WHO/ECDC); weighting not published; African coverage depth unquantified	**2**	Functional annotation databases described in Balaji et al. (2022); LMIC-endemic pathogen representation not quantified or disclosed
Output explainability	**2**	Dashboard shows triggering articles for authorised users; no confidence scoring; alert prioritisation reasoning not disclosed	**2**	FunSoC outputs interpretable by trained bioinformaticians; no plain-language output for non-expert or LMIC users
Performance reporting	**1**	COVID-19 pre-detection documented; no sensitivity/specificity data disaggregated by WHO AFRO sub-region or disease type	**2**	Precision/recall published in Balaji et al. (2022) and disclosed in 2024 red-teaming study; no LMIC-specific validation
Language accessibility	**2**	Multi-language article ingestion; interface in UN official languages; African language depth (Swahili, Hausa, Amharic) not documented	**1**	English-only interface and documentation; no non-English user support documented
ACCOUNTABILITY ⚠ Override Clause Dimension — a score of 0 on any sub-dimension triggers Low Governance Readiness				
Developer accountability	**3**	WHO governed by 194 member states via Executive Board; WHO Evaluation Policy revised June 2025 — structured intergovernmental accountability	**2**	Rice University and Signature Science LLC; named PIs documented; accountability via academic publication only; no formal legal liability
Regulatory oversight ★	**0 ★**	WHO IS the regulator — no independent authority oversees EIOS algorithmic operations; not classified under any national AI framework	**0 ★**	Not subject to any binding governance framework in any jurisdiction; not covered by ISO 20688-2:2024; OSTP 2024 Framework was non-mandatory
Incident reporting ★	**1**	IHR Art. 6 governs member-state reporting; no published protocol for EIOS algorithmic failure escalation; Dec 31 2019 detection gap never formally investigated	**0 ★**	No formal incident reporting mechanism; no obligation for synthesis providers to report when a SeqScreen-flagged order proceeds (Wheeler et al., 2024)

Sub-dimension	EIOS	EIOS — Key Finding	SeqScreen	SeqScreen — Key Finding
Independent audit	1	Academic peer review by MacIntyre et al. (2023) and Villanueva-Miranda et al. (2025); no formal independent technical audit of EIOS AI system	1	Peer review in Genome Biology (Balaji et al., 2022); not included in the four-tool Wittmann et al. (2025) red-team study; no independent audit
Redress mechanisms ★	0 ★	No formal process for African governments to challenge incorrect EIOS alerts, failures to escalate, or systematic blind spots	0 ★	No formal redress mechanism for any affected government, institution, or population from a missed screening or false flag (Pannu et al., 2025)
EQUITY				
Access equity	1	Restricted to 120 designated governments; NGOs, academic institutions, and civil society cannot access EIOS directly	3	Free, open-source globally; no cost, no registration, no institutional affiliation required — lowest access barrier of both tools
Geographic coverage	2	120+ countries monitored; rural Africa, conflict-affected areas, and pastoral communities systematically underrepresented due to reliance on internet media	1	Limited to providers with internet connectivity and bioinformatics capacity; regulatory-list pathogens may not capture Lassa fever or Marburg
Data representativeness	1	Relies on internet news media; structural underrepresentation of rural Africa, conflict areas, and communities with limited press freedom	1	Standard international sequence databases used for training; LMIC-endemic pathogen representation not audited or published
Benefit distribution	2	47 WHO AFRO states receive alerts; signal-to-action gap — early warning without response capacity cannot reduce mortality	1	Current benefit minimal where no commercial-scale African DNA synthesis providers operate; benefit will grow as Africa's bioeconomy develops
Governance participation	2	African states vote in WHO governance; no African institution co-develops EIOS AI systems; WHO Hub Berlin leads all technical development	0	U.S.-only academic consortium (Rice/Signature Science); no LMIC co-developers; no formal LMIC voice in governance or development decisions
DATA GOVERNANCE				
Data ownership	1	WHO-owned aggregated surveillance data; member-state data sovereignty within EIOS not explicitly defined in published documents	3	Runs locally — no data transmitted to developers; data ownership remains entirely with the deploying institution — strongest posture of both tools
Sovereignty protections	1	IHR data reporting obligations exist; no specific data sovereignty framework for EIOS-generated surveillance intelligence	3	Local operation protects IP and sequence data from external exposure by design; no raw sequence data leaves provider infrastructure
Cross-border sharing rules	2	Integrates global feeds (ProMED, HealthMap, GPHIN, JHU); no published consent framework governing how third-party source data is aggregated	3	No cross-border data sharing; local processing by design — strongest cross-border data protection of both tools
Benefit-sharing	0	No documented benefit-sharing arrangements for countries and	0	No benefit-sharing arrangements for LMIC data contributors; no mechanism to share

Sub-dimension	EIOS	EIOS — Key Finding	SeqScreen	SeqScreen — Key Finding
		populations whose surveillance data is ingested and processed by EIOS		screening improvements with LMIC institutions
Consent and re-use	**1**	WHO data governance policies exist generally; no EIOS-specific consent or re-use limitation document published for aggregated surveillance data	**1**	Open-source MIT-style licence; no specific re-use limitations for screened sequence data or flagging records documented
DUAL-USE RISK (★ Biological misuse potential is an override trigger)				
Biological misuse potential ★	**3**	No genetic sequence data processed; restricted to designated governments; geopolitical misuse risk (diplomatic exploitation of early outbreak signals) limited	**2**	Defensive tool by design; however open-source architecture creates adversarial reverse-testing vulnerability — any actor can test evasion before ordering synthesis
Screening for dangerous outputs	**3**	Not applicable: EIOS monitors open-source news media and does not generate or screen biological sequences	**3**	Core function: identifies sequences of concern using FunSoCs — detects dangerous biological function regardless of taxonomic origin
Adversarial testing	**1**	No published red-teaming or adversarial evaluation of EIOS AI classification systems	**1**	No published adversarial evaluation of SeqScreen's resilience to AI-generated evasive sequences
Access controls	**2**	Access restricted to designated governments via WHO AFRO intermediary; layered access model reduces direct misuse risk	**1**	Open-source with no access controls; any actor can download SeqScreen and test whether planned sequences evade detection
SUSTAINABILITY				
Local operation	**1**	Cloud-hosted WHO infrastructure; no local hosting option for member states; dependent on WHO Hub Berlin	**3**	Runs locally on standard hardware; no cloud dependency; works in low-connectivity settings
Local expertise	**2**	WHO AFRO provides training; variable capacity across 47 WHO AFRO states	**1**	Command-line interface requiring bioinformatics expertise; no GUI; significant technical capacity barrier for LMIC synthesis providers
Long-term financing	**3**	Backed by WHO institutional budget and EIOS Strategy 2024–2026 co-funded by Germany; multi-source funding reduces single-funder dependency	**1**	Academic and grant-funded via Rice University and Signature Science; no guaranteed long-term institutional support
Local adaptability	**0**	Cannot be modified by local institutions without WHO permission; African NPHIs are end-users, not co-developers	**3**	Fully open-source; local institutions can legally and technically modify and maintain the tool without requiring external permission
Technology dependency	**1**	Dependent on WHO Hub Berlin cloud infrastructure and contracted data providers; African member states have no independent maintenance capacity	**3**	No cloud dependency; runs entirely on local infrastructure; no dependence on external APIs or proprietary databases
RAW SCORE / MAX	**54 / 102 (53%)**		**55 / 102 (54%)**	

Sub-dimension	EIOS	EIOS — Key Finding	SeqScreen	SeqScreen — Key Finding
OVERRIDE TRIGGERS	**2 triggers: Regulatory oversight (0) + Redress mechanisms (0)**		**3 triggers: Regulatory oversight (0) + Incident reporting (0) + Redress mechanisms (0)**	
FINAL CLASSIFICATION	**LOW GOVERNANCE READINESS**		**LOW GOVERNANCE READINESS**	

Note: Override Clause - Raw percentage scores (EIOS 53%; SeqScreen 54%) would suggest Moderate Governance Readiness. The Override Clause reclassifies both tools as Low Governance Readiness because critical Accountability sub-dimensions score 0. A score of 0 on Regulatory oversight, Incident reporting, or Redress mechanisms cannot be compensated by stronger performance elsewhere. The override reflects the principle that governance which cannot be enforced, audited, or challenged is not governance.

8.3 Comparative Analysis and Override Implications

Both tools receive a final classification of Low Governance Readiness, triggered by the Override Clause rather than by low raw scores. This is analytically significant: it means both tools have genuine technical strengths that would appear adequate in a simple percentage-based assessment. The Override Clause reveals what percentage scores conceal that accountability failures cannot be compensated by strong performance elsewhere.

EIOS and SeqScreen address entirely different biosurveillance functions, outbreak intelligence and sequence screening respectively yet share the same critical governance deficit: neither is subject to binding regulatory oversight, neither has formal incident reporting requirements, and neither provides affected governments or populations with any mechanism to challenge outputs or seek redress. The tools are different; the accountability gap is identical.

For Africa and LMICs specifically, the override findings carry direct practical implications. EIOS alerts reaching 47 WHO AFRO member states come from a system whose AI classification logic is unpublished and has not been subject to any published independent technical audit, with no formal process for those governments to challenge incorrect alerts or systematic blind spots. SeqScreen, while free and locally operable, offers LMIC institutions no governance participation, no benefit-sharing from the tool's ongoing development, and no regulatory protection when its screening fails. Both tools therefore impose a governance risk on LMIC users that raw percentage scores alone would obscure, a risk the Override Clause is specifically designed to surface.

9. Africa and LMIC Governance Landscape

9.1 Regional actor map

Table 7: Africa Regional Biosurveillance Landscape

Region	Key Countries/Actors	Key Stakeholders	Surveillance Role & AI Governance Relevance
West Africa	Ghana, Nigeria, Senegal, Sierra Leone	Africa CDC, ACEGID, WHO AFRO, Institut Pasteur Dakar, WAHO	Genomic surveillance for Lassa fever, Ebola, Mpox. ACEGID provides data to global AI systems without co-governance rights. Institut Pasteur Dakar is a WHO reference centre for arboviruses
East Africa	Uganda, Kenya, Rwanda, Ethiopia	KEMRI-Wellcome, Africa CDC, WHO AFRO, SACIDS, Ministries of Health	Pathogen genomics, outbreak detection, AI-enabled surveillance. KEMRI-Wellcome is the core East Africa node - Wellcome Trust funding dependence creates sustainability risk
Southern Africa	South Africa, Zambia, Malawi, Mozambique	NICD, H3ABioNet, national genomics programs, SACIDS	NICD leads AI biosurveillance across the continent. H3ABioNet provides the bioinformatics backbone across 30+ institutions. Sequencing capacity is most advanced here but not evenly distributed
Central Africa	Cameroon, DRC	Public health institutes, WHO AFRO, SACIDS, regional laboratories	Outbreak surveillance for high-consequence pathogens (Ebola, Mpox). Weakest AI biosurveillance infrastructure relative to disease burden.

North Africa	Morocco, Egypt, Tunisia	Universities, ministries, ACEGID network, Institut Pasteur network	Public health intelligence and genomic surveillance expansion. Growing AI capacity in academic institutions; governance frameworks at early stages

9.2 Key Governance Challenges

Four structural challenges characterise Africa's AI biosurveillance governance landscape. First, most African countries lack integrated legal and ethical frameworks for AI-supported surveillance, cross-border genomic data sharing, and dual-use biosecurity oversight. Second, genomic data generated by African populations are frequently extracted and incorporated into AI systems developed and owned by external institutions, with limited benefit-sharing or local control (Munung et al., 2024; Thaldar, 2024). Third, the signal-to-action gap, early warnings reaching governments that lack the response capacity to act, means tools like EIOS may improve detection without reducing mortality. Fourth, African institutions are not co-developers of any of the 23 tools in this review, meaning Africa participates as a deployment context but not as a governance actor in the tools that surveil its populations.

Africa CDC's health data governance Flagship Initiative and the 2025–2030 Biosafety and Biosecurity Strategy represent important inflection points. Long-term sustainability will depend on strengthening local computational infrastructure, workforce capacity, ethical oversight, and national ownership of genomic data systems (Rebai et al., 2025; Africa CDC, 2025).

10. Recommendations and implications

The governance gaps identified in this study reflect structural features of the current international governance landscape that apply across the full catalogue of twenty-three tools examined and, by extension, to any AI-enabled biological threat detection system deployed today. AI-enabled biological detection tools are no longer a technical supplement to public health systems; they are a critical global security infrastructure with implications for national sovereignty, economic stability, and catastrophic risk prevention. Five priority recommendations follow, addressed to the actors best positioned to close each gap.

1) For international governance bodies: extend and enforce the regulatory perimeter for AI-enabled biological systems. The STAE+ AIxBiosecurity Governance Readiness framework for AI-enabled biodetection tools can be utilized before deployment deployment of tools.
2) Regional bodies and data contributing member states: stablish and strengthen regional federated data platforms for pathogen genomics that preserve national data sovereignty and enforce benefit-sharing
3) National governments and regional bodies**:** use the STAE+ Governance Readiness Framework as a procurement, regulatory, and legislative instrument. Applied at the procurement stage, it provides a structured basis for demanding transparency documentation, data sovereignty protections, and benefit-sharing arrangements as scored conditions rather than informal requests. Applied legislatively, it offers a template for national AI biosecurity regulation. African and LMIC governments in particular can use it to set terms for tool deployment within their jurisdictions.
4) Developers of AI biological detection tools: treat transparency, accountability, and access governance as design requirements, not an afterthought.
5) Research and AI safety community**:** redirect attention toward biological AI governance as a priority domain distinct from model alignment or misinformation. Empirical comparative studies of AI biological detection tools governance across countries, and analysis of how biological AI systems are being deployed in public and private sectors, would strengthen the evidence base governance reform requires. This analysis demonstrates that biological applications require governance attention distinct from existing AI safety discourse focused on misinformation, autonomous systems, or model alignment. The specific governance failures identified here, unaudited algorithmic operations, absent incident reporting, no redress mechanisms, no benefit-sharing are not problems that model alignment addresses.

Several questions remain unresolved. How governance systems can balance rapid innovation with precaution during public health emergencies where delays may cost lives remains unclear. Questions also remain regarding enforcement, and how LMICs can participate equitably in AI-enabled bio surveillance without becoming

dependent on externally controlled infrastructures is the deepest question this study raises. Addressing it will require governance architectures that treat equity not as an aspirational add-on but as a foundational design requirement from the outset.

11. Conclusion

AI-enabled biological threat detection is rapidly transforming global health surveillance and biosecurity, but governance systems have not evolved at the same pace as the technologies they are intended to regulate. This paper has argued that current frameworks remain fragmented and insufficient to address the ethical, political, and security challenges emerging at the intersection of artificial intelligence, biological data systems, and global health security.

The STAE+ Governance Readiness Framework developed in this study operationalises four governance principles, transparency, accountability, equity, and shared security into seven evaluable dimensions and thirty-four scored sub-dimensions, providing a structured and replicable instrument for assessing any AI-enabled biological threat detection tool against a consistent evidence-based standard. Applied to WHO EIOS and SeqScreen, the framework reveals that both tools, despite genuine technical strengths and raw scores suggesting moderate adequacy, are correctly classified as Low Governance Readiness once the override clause is applied to their critical accountability failures. Neither tool is subject to binding regulatory oversight in any jurisdiction. Neither provides formal mechanisms for affected governments or populations to challenge its outputs. These are not technical deficiencies, they are governance design choices that can and should be corrected.

The framework's value extends beyond this study. National governments can apply to develop national AI biosecurity regulations. Regional bodies such as the Africa CDC can embed it within continental health data governance frameworks. Developers can use it to identify and address governance gaps before deployment rather than after. International bodies can draw on its dimensions to inform treaty provisions, procurement standards, and audit requirements. It is designed for use as a practical instrument for the governance reforms this paper argues are necessary and urgent.

As AI systems become more deeply integrated into biological data surveillance infrastructures, the future of global biosecurity will depend not only on technological innovation, but also on the ability of governments, institutions, and international organizations to govern these systems responsibly and inclusively.

12. References

Ahdritz, G., Bouatta, N., Floristean, C., Kadyan, S., Xia, Q., Gerecke, W., O'Donnell, T. J., Berenberg, D., Fisk, I., Zanichelli, N., Zhang, B., Nowaczynski, A., Wang, B., Stepniewska-Dziubinska, M. M., Zhang, S., Ojewole, A., Guney, M. E., Biderman, S., Watkins, A. M., … AlQuraishi, M. (2024). OpenFold: Retraining AlphaFold2 yields new insights into its learning mechanisms and capacity for generalization. Nature Methods, 21(8), 1514–1524. https://doi.org/10.1038/s41592-024-02272-z

Africa CDC. (2025). Africa's new five-year plan for biosafety and biosecurity. https://africacdc.org/news-item/africas-new-five-year-plan-for-biosafety-and-biosecurity/

Arms Control Association. (2025, November 24). Regulatory gaps in benchtop nucleic acid synthesis create biosecurity vulnerabilities. https://www.armscontrol.org/blog/2025-11-24/regulatory-gaps-benchtop-nucleic-acid-synthesis-create-biosecurity-vulnerabilities

Balaji, A., Kille, B., Kappell, A. D., Godbold, G. D., Diep, M., Elworth, R. A. L., Qian, Z., Albin, D., Nasko, D. J., Shah, N., Pop, M., Segarra, S., Ternus, K. L., & Treangen, T. J. (2022). SeqScreen: Accurate and sensitive functional screening of pathogenic sequences via ensemble learning. Genome Biology, 23(1), 133. https://doi.org/10.1186/s13059-022-02695-x

Brownstein, J. S., Freifeld, C. C., Reis, B. Y., & Mandl, K. D. (2008). Surveillance sans frontières: Internet-based emerging infectious disease intelligence and the HealthMap project. PLOS Medicine, 5(7), e151. https://doi.org/10.1371/journal.pmed.0050151

Bulletin of the Atomic Scientists. (2024, November). What will be the impact of AI on the bioweapons treaty? https://thebulletin.org/2024/11/what-will-be-the-impact-of-ai-on-the-bioweapons-treaty/

Carrion, M., & Madoff, L. C. (2017). ProMED-mail: 22 years of digital surveillance of emerging infectious diseases. International Health, 9(3), 177–183. https://doi.org/10.1093/inthealth/ihx014

Adamson, G., & Allen, G. C. (2025). Opportunities to strengthen U.S. biosecurity from AI-enabled bioterrorism: What policymakers should know. Center for Strategic and International Studies. https://www.csis.org/analysis/opportunities-strengthen-us-biosecurity-ai-enabled-bioterrorism-what-policymakers-should

Federation of American Scientists. (2024). Bio x AI: Policy recommendations for a new frontier. https://fas.org/publication/bio-x-ai-policy-recommendations/

Giordano, J. (2025). Biotechnologies and the treaty gap: Why biological weapons governance is falling behind. National Defense University Strategic Insights. https://digitalcommons.ndu.edu/strategic-insights/43/

International Biosecurity and Biosafety Initiative for Science. (2024). International screening standards. https://ibbis.bio/our-work/international-screening-standards/

MacIntyre, C. R., Chen, X., Kunasekaran, M., Quigley, A., Lim, S., Stone, H., Paik, H., Yao, L., Heslop, D., Wei, W., Sarmiento, I., & Gurdasani, D. (2023). Artificial intelligence in public health: The potential of epidemic early warning systems. Journal of International Medical Research, 51(3). https://doi.org/10.1177/03000605231159335

Munung, N. S., Thaldar, D., Andanda, P., Kerr, R., Herbst, K., Mabuka, J., Wamuyu, R., Bukini, D., & Dandara, C. (2024). Genomics and health data governance in Africa: Democratize the use of big data and popularize public engagement. Hastings Center Report. https://doi.org/10.1002/hast.4933

National Academies of Sciences, Engineering, and Medicine. (2025). The age of AI in the life sciences: Benefits and biosecurity considerations. National Academies Press. https://www.ncbi.nlm.nih.gov/books/NBK614605/

Nuclear Threat Initiative. (2024). Exploring AI-biosecurity governance in the Global South. https://www.nti.org/risky-business/exploring-ai-biosecurity-governance-in-the-global-south/

OECD. (2025). Synthetic biology, AI and automation: A forward-looking technology assessment (OECD Science, Technology and Industry Policy Papers, No. 187). https://doi.org/10.1787/12158721-en

Pannu, J., Bloomfield, D., MacKnight, R., Hanke, M. S., Zhu, A., Gomes, G., Cicero, A., & Inglesby, T. V. (2025). Dual-use capabilities of concern of biological AI models. PLOS Computational Biology, 21(5), e1012975. https://doi.org/10.1371/journal.pcbi.1012975

Parums, D. V. (2025). Editorial: The 2025 World Health Assembly pandemic agreement and the 2024 amendments to the International Health Regulations. Medical Science Monitor. https://pmc.ncbi.nlm.nih.gov/articles/PMC12228423/

Rebai, A., Abayomi, A., Andanda, P., Kerr, R., Herbst, K., Mabuka, J., Wamuyu, R., Bukini, D., & Dandara, C. (2025). Responsible governance of genomics data and biospecimens in Africa. BMJ Global Health, 10(2), e016026. https://doi.org/10.1136/bmjgh-2024-016026

Thaldar, D. (2024). Editorial: Data governance in African health research: ELSI challenges and solutions. Frontiers in Pharmacology. https://doi.org/10.3389/fphar.2024.1525434

Villanueva-Miranda, I., Xiao, G., & Xie, Y. (2025). Artificial intelligence in early warning systems for infectious disease surveillance: A systematic review. Frontiers in Public Health, 13, 1609615. https://doi.org/10.3389/fpubh.2025.1609615

Wheeler, N. E., Carter, S. R., Alexanian, T., Isaac, C., Yassif, J., & Millet, P. (2024). Developing a common global baseline for nucleic acid synthesis screening. Applied Biosafety. https://doi.org/10.1089/apb.2023.0034

Wittmann, B. J., Alexanian, T., Bartling, C., Beal, J., Clore, A., Diggans, J., Flyangolts, K., Gemler, B. T., Mitchell, T., Murphy, S. T., Wheeler, N. E., & Horvitz, E. (2025). Strengthening nucleic acid biosecurity screening against generative protein design tools. Science, 390, 82–87. https://doi.org/10.1126/science.adu8578

World Health Organization. (2021). Ethics and governance of artificial intelligence for health. https://www.who.int/publications/i/item/9789240084759

World Health Organization. (2024a). EIOS initiative: Strategy 2024–2026. https://www.who.int/initiatives/eios

World Health Organization. (2024b). International Health Regulations (2005), as amended in 2014, 2022 and 2024. https://apps.who.int/gb/bd/pdf_files/IHR_2014-2022-2024-en.pdf

World Health Organization. (2025). WHO pandemic agreement — Questions and answers. https://www.who.int/news-room/questions-and-answers/item/pandemic-prevention--preparedness-and-response-accord

World Health Organization. (2026, February 2). Six years after COVID-19's global alarm: Is the world better prepared? https://www.who.int/news/item/02-02-2026-six-years-after-covid-19-s-global-alarm-is-the-world-better-prepared-for-the-next-pandemic