CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

MARCH 2026

Kenya's Health Deal Is a Stress Test for the America First Global Health Strategy

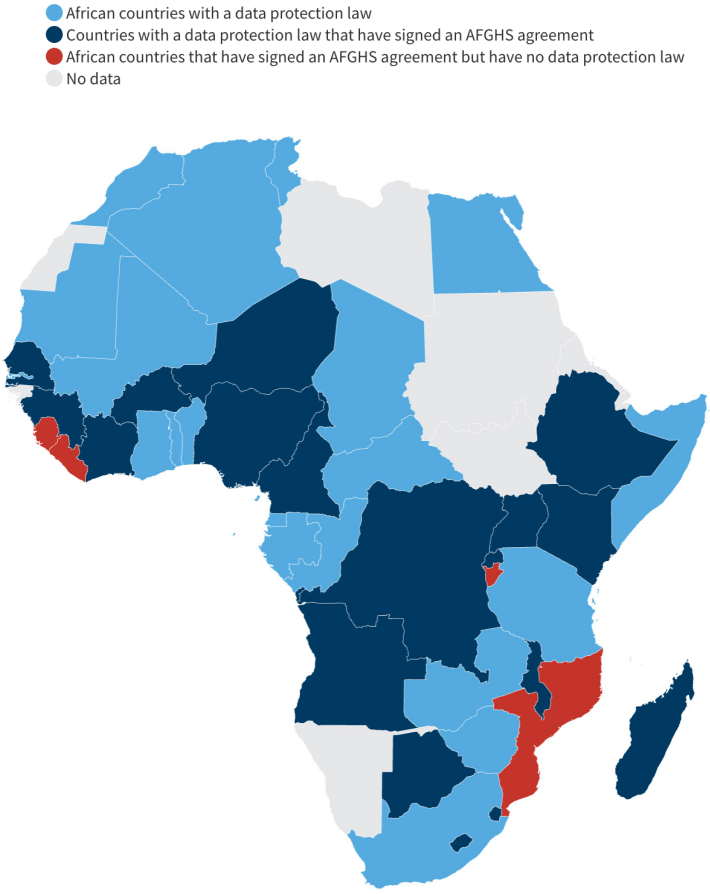
Jane Munga and Rose Mosero

In the span of three months starting late last year, twenty-two African countries signed bilateral agreements on global health cooperation with the United States under its America First Global Health Strategy (AFGHS). The AFGHS signals a fundamental recalibration of U.S. global health policy toward bilateralism anchored in strategic alignment to President Donald Trump's vision of making America safer, stronger, and more prosperous. The global health–related bilateral agreements are foreign policy instruments for forwarding this vision with countries that receive U.S. health assistance. They aim to strengthen bilateral ties, maximize the impact of U.S. health aid, and promote U.S. health innovation. At their core, the agreements seek to save lives by stopping the spread of diseases globally and preventing outbreaks from reaching U.S. shores.

Achieving this ambition depends on disease surveillance and monitoring capabilities availed by health systems powered by a continuous flow of health data. This makes access and sharing of health data central to AFGHS implementation. However, health data is not like any other data. Defined by the World Health Organization (WHO) as "raw, unprocessed numbers, measurements, that relate directly to the health and well-being status of an individual or to the health services that the individual receives," health data is regarded and classified as sensitive personal data and is subject to heightened legal protections globally. It is protected and carries strategic significance—it is a technical input yet also a national asset, with implications for countries' sovereignty and long-term value creation.

Across Africa, countries have adopted—revealed through the Africa Technology Policy Tracker—comprehensive data protection and privacy regimes to assert national control over how personal data is collected, processed, and shared. This is mostly seen through the enactment of data protection laws (see figure 1). Increasingly, governments are also safeguarding citizens' data as a sovereign national resource, driven by the view that control over data—and the infrastructure that manages it—confers influence over the digital economy and its associated commercial and strategic advantages. Kenya in particular has actively championed data sovereignty by explicitly identifying data as a strategic national asset, to be safeguarded for national interests. The importance of data sovereignty by African countries has been surfaced by the U.S. pursuit of bilateral AFGHS agreements.

Figure 1. African Countries with Data Protection Laws and America First Global Health Strategy Agreements



Source: Africa Technology Policy Tracker, America First Global Health Strategy

Kenya was the first African country to sign a bilateral agreement with the United States under the AFGHS, but since then, the agreement has been halted by Kenyan courts. A petition filed with the court argued that the framework violated Kenya's constitutional safeguards on privacy and transparency and breached data protection and digital health statutes by permitting broad foreign access to sensitive health data. Kenya's case regarding its AFGHS agreement offers an early and revealing test of the U.S. model for global health cooperation. This model has recently been questioned in Zimbabwe, which rejected the health deal due to data sharing concerns, and in Zambia, which raised questions on the data-sharing clauses (among other issues) during negotiations. These cases demonstrate how domestic legal frameworks and evolving understandings of data sovereignty can influence global health cooperation and suggest that AFGHS agreements may require recalibration to better account for health data protections in partner countries.

Policy Friction: When AFGHS Meets Sovereignty

According to the U.S. Department of State, the bilateral agreements are designed to "advance a comprehensive and shared vision directly between the United States and recipient country governments for continued future cooperation on global health issues," with implementation set to begin in April 2026. The Trump administration underscores that this design responds to critiques of global health assistance, including inefficiency and waste, fragmentation, donor dependence, and weak national ownership. By negotiating directly with partner governments, Washington seeks to embed its America First health agenda through a standardized implementation template that includes:

1. **Funding frontline commodities and healthcare workers.** The United States will maintain full funding for essential medical commodities—such as diagnostics, drugs, vaccines, and related supplies—as well as the salaries of frontline health workers currently supported by U.S. health assistance programs for the next year. After the 2026 fiscal year, partner governments are expected to gradually integrate these costs into national health budgets, with the pace of transition calibrated to each country's income level.

2. **Establishing integrated health data systems.** Countries will develop streamlined monitoring systems capable of tracking epidemiological trends,

service delivery outcomes, and supply chain performance across major disease programs (such as HIV/AIDS, malaria, tuberculosis, and polio). These systems aim to replace fragmented, disease-specific reporting structures while enabling the long-term data sharing needed for outbreak surveillance, program management, and statutory reporting.

3. **Transitioning technical assistance toward government ownership.** U.S. support will shift away from directly managing individual clinical sites toward strengthening government capacity to manage key program functions. This shift includes greater reliance on government-to-government assistance and partnerships with faith-based service providers and the private sector. The private sector would be engaged in the procurement and distribution of health commodities, service delivery, and data systems—utilizing off-the-shelf, private sector solutions instead of fully government-designed and -managed data systems.

4. **Introducing coinvestment and performance benchmarks.** Recipient governments will be required to contribute financially to program delivery and meet agreed service and outcome targets. Progress against these benchmarks will determine whether subsequent tranches of U.S. health assistance funding are released.

This template not only places health data at the center of implementation but also inadvertently transforms it into a necessary lever to verify results and unlock funding.

In Kenya, friction has emerged at the intersection of the bilateral Cooperation Framework's data provision with national laws, constitutional safeguards, and public scrutiny. Kenya's High Court halted implementation of the AFGHS agreement pending the hearing of a case challenging its legality. Petitioners argue that the framework contravenes Kenya's data protection laws and was negotiated without adequate public participation or parliamentary oversight. In response, the court granted an injunction, finding that the petition raised credible legal questions and ordering a pause in implementation until the matter is fully examined.

The ruling offers an early and consequential stress test of the AFGHS model. It also reflects a broader tension as governments increasingly assert greater control over cross-border access to and use of sensitive national data. This raises a fundamental question for Washington and African leaders alike: Can AFGHS agreements become durable foreign policy anchors while remaining compatible with domestic legal frameworks that assert data sovereignty?

The Case of Kenya: An Early Warning Signal

Against this backdrop of data protection, cross-border data regulation, and sovereignty concerns, Kenya provides an instructive case for how data governance is being asserted in practice. The country has taken several steps to protect data sovereignty:

- Developed a robust data protection **regulatory framework**, including the Data Protection Act, 2019
- Passed **sector-specific legislation**, including a Digital Health Act, 2023
- Established an independent **data protection authority**—The Office of the Data Protection Commissioner—with an active adjudication process

Together, these legal and institutional measures reflect a policy posture aimed at safeguarding Kenyans' personal data. This approach has been reinforced through high-profile enforcement actions, including the suspension of Worldcoin operations in 2023. Worldcoin, an entity linked to OpenAI's CEO Sam Altman, brought issues of data protection into sharp focus after collecting biometric

data from around 300,000 Kenyans through its Orb devices, as part of its efforts to build its World ID. In 2025, a Kenyan court ruled that the project contravened the Data Protection Act, prohibited the company from collecting or processing biometric data in the country, and ordered the deletion of all Kenyan data previously collected.

It is no surprise therefore that the U.S.-Kenyan Health Cooperation Framework has received heightened scrutiny in Kenya's regulatory ecosystem. While the agreement appears, on the surface, to be a routine instrument for health collaboration, a closer reading has revealed a more consequential text. The data sharing agreement (particularly the section "Provision of Data to U.S. Government") institutionalizes foreign access to Kenyan health data and biological materials, including access to national health information systems (such as surveillance systems, electronic medical records, and warehouse management platforms) and the sharing of genomic and pathogen data. This has significant implications for data governance, national control, and benefit sharing.

Without such arrangements, countries risk becoming primarily suppliers of valuable data while the economic and technological value derived from it accrues elsewhere.

To be sure, the Government of Kenya has stated that only aggregated and anonymized data will be shared under the framework. However, in today's data environment, that assurance is increasingly difficult to sustain. Large datasets, particularly health datasets, can often be reidentified through linkages with other data sources or through advanced analytics and AI. Empirical studies have shown multiple instances where supposedly deidentified hospital and claims datasets were successfully linked back to named individuals. As a result, the distinction between identifiable and unidentifiable data becomes blurred, leading to a potential loss of effective control over some of Kenya's most sensitive data.

The concern is not merely about technical language but also about sovereignty. In the digital era, data sovereignty is about more than where data sits or who formally owns it; it is also about who has the power to decide how data is accessed, used, stored, retained, and reused. By creating standing mechanisms for external access to health and biological data—without clear, enforceable safeguards and limits—the AFGHS framework poses significant risks that constrain Kenya's future data autonomy. This concern is heightened by the strategic value of health and biological data for AI development, pharmaceutical research and development, and broader innovation and manufacturing processes.

This strategic value raises an additional and unresolved question: **How do countries benefit from the use of the data they provide?** This question has taken center stage in global health governance—framed through the lens of **benefit sharing**. Benefit sharing refers to mechanisms through which countries that provide pathogen samples, genomic data, or health datasets participate in the scientific, technological, and economic gains generated from that data's use. Benefits can include access to resulting vaccines, therapeutics, and diagnostics; technology transfer and local research partnerships; investments in national data infrastructure; or participation in downstream manufacturing and innovation ecosystems. Without such arrangements, countries risk becoming primarily suppliers of valuable data while the economic and technological value derived from it accrues elsewhere.

In fact, these concerns have become a central point of contention in international governance frameworks. Some observers have argued that the AFGHS template overrides the World Health Organization's proposed Pandemic Agreement and its Pathogen Access and Benefit Sharing (PABS) framework and instead seeks to develop a parallel global surveillance system. However,

the WHO's framework includes explicit provisions governing how countries will share in the benefits derived from the provision of pathogen information, genetic data, and other materials—provisions that the AFGHS omit. Notably, before it fully withdrew from the WHO, the United States rejected the PABS amendment, arguing that such data sharing infringed on its own sovereignty.

Tensions Within Kenya's Framework

The concern about data sovereignty hinges on the fact that the AFGHS agreement does not explicitly prohibit the use of Kenyan pathogen data for purposes beyond health cooperation (but neither does it authorize it). In the absence of clear, enforceable limits, the agreement relies on broad statements of intent. It contains no binding restrictions on secondary or downstream use, provides no clear limits on onward sharing the data with other parties, and offers no safeguards against the data being combined with other datasets once it leaves Kenya's control. This opens the door to interpretations under which Kenyan health and pathogen data could be repurposed for activities beyond outbreak response or public health cooperation. For example, such data could be used in pharmaceutical or biotechnology research, incorporated into large-scale biomedical datasets used to train AI models, or shared with third-party research institutions and private sector actors (as already alleged) without Kenya's knowledge or participation. In these scenarios, Kenyan datasets could contribute to commercially valuable innovations—including vaccines, therapeutics, diagnostics, or data-driven health technologies—while Kenya itself has no guaranteed access to the resulting products, intellectual property, or economic returns.

The design of the U.S.-Kenya Health Cooperation Framework appears to be at odds with Kenya's legal frameworks, first within the legal text and second through process failures.

Agreement Text

The Data Protection Act, 2019, classifies health data as sensitive personal data and provides stringent parameters for its cross-border transfers. Importantly, transfers are only allowed where there are sufficient protections in place or where existing legal protections are in place, usually subject to the Office of the Data Protection Commissioner's oversight. While such international arrangements are provided for under Kenya's Data Protection Regulations (a set of subsequent regulations that provide clear guidance on data sharing), they require clear, reciprocal data protection safeguards. The U.S.-Kenya framework, however, shows little provision for safeguards. In the absence of a reciprocal agreement, the regulations impose localization requirements mandating that health data related to the provision of both primary and secondary healthcare services be stored or processed on servers located within Kenya.

The Digital Health Act, 2023, reiterates this national position on the localization of health data. Under the act, health data must be stored in Kenya, and transfers outside Kenya are permissible only under certain prescribed conditions, particularly in cases of health tourism. Routine data sharing, as envisaged under the agreement, appears to fall outside of the exceptions permitted by the Digital Health Act.

These legal concerns were articulated in a petition filed on December 10, 2025, in *Okiya Omtatah Okoiti v. Ministry of Foreign Affairs and International Trade*. The petition argued that the framework violated Kenya's constitutional safeguards on privacy and transparency, breached data protection and digital health statutes by permitting broad foreign access to sensitive health data, and lacked parliamentary fiscal approval for the government's $850 million spending commitment. The High Court first suspended all data-sharing provisions of the U.S.-Kenya agreement and later extended the suspension to the entire agreement. These rulings served as a strong judicial reminder that international health cooperation cannot proceed outside the framework of

domestic law and offer an early and consequential stress test on data-sharing provisions of the AFGHS.

Additionally, the lack of clear benefit-sharing provisions, despite Kenya's support for PABS during the WHO treaty negotiations, leaves the country in a vulnerable position. With benefit sharing left to be negotiated later and on a case-by-case basis, Kenya's agency may be diminished in securing fair terms especially when faced with urgent funding needs or limited leverage. This raises real concerns about whether the country will truly benefit from the data and biological resources it provides and if the WHO international governance model in the end will prevail over bilateral arrangements. These facts lead to an important takeaway: The Kenya AFGHS positions Kenya as largely a data supplier, while value creation may occur elsewhere. This has prompted nearly fifty civil society organizations to warn that the arrangements risk entrenching data-extractive dynamics.

Process Failures

The agreement was further complicated by process failures. The Cooperation Framework that secured $1.6 billion for Kenya's health programs was negotiated without publicly disclosing its terms, informing stakeholders, or allowing affected communities, civil society, or oversight bodies to provide input on or assess its implications—especially with respect to health data sharing. This raised a legal challenge to the agreement's constitutionality, as decisions involving sensitive health data and privacy rights demand greater transparency and discussion. The Kenya agreement was publicly communicated only after it was signed and public outcry had already emerged, turning the process from engagement into justification.

Further, by the Kenyan governmental neglect of parliamentary oversight and public participation, the framework's legitimacy was compromised, leading to litigation and a possible erosion of public trust not only in the agreement but also in the institutions involved. This position was raised in court as well as in public criticisms by civil society actors and Kenya's netizens, who flooded social media questioning the deal. The High Court ultimately found the procedural discrepancies compelling enough to suspend the entire agreement, holding that it must "have an opportunity to interrogate the tissues [sic] raised and determine not only the constitutionality but also the legality of the Framework."

Lingering Policy Friction

More broadly, the U.S.-Kenya framework illustrates how capacity building and an ownership-focused framework can coexist with equity and sovereignty concerns. While the Kenya agreement includes substantive provisions aimed at reducing donor dependency and strengthening national ownership of health system operations, it lacks binding commitments on benefit sharing and technology transfer linked to Kenya's genomic data, leaving questions about long-term control and use unresolved. The subsequent Data Sharing Agreement—introduced as an annex to the Cooperation Framework in response to public outcry—references the Data Protection Act and Digital Health Act and signals an intent to align with domestic legal frameworks. However, the agreement's vague language and absence of enforceable safeguards appear to fall short of Kenya's statutory requirements on access controls, data protection, and data minimization, thereby constraining Kenya's ability to exercise meaningful data sovereignty.

Kenya's legal processes have effectively paused implementation of the country's AFGHS, leaving the timeline for operationalization and associated funding flows uncertain. A similar concern is noted in Zambia, where benefit-sharing concerns have emerged and delayed the signing of the agreement. AFGHS negotiators reportedly raised questions about committing to data sharing for up to twenty-five years in exchange for assistance provided over only five years.

The Way Ahead

The AFGHS bilateral agreements follow a standardized template. If weaknesses around health data governance and public consultation are embedded in that template, Kenya's response may have a demonstration effect. Most other African countries that have signed the agreements also have data protection laws, meaning similar legal tensions could emerge elsewhere. For African stakeholders, the question is not whether cooperation is desirable, but whether each agreement is grounded in a clear legal basis and genuinely reflects the regulatory realities of the partner country. Where bargaining power is uneven, there is a real risk that critical legal principles, such as data protection, public participation, or benefit sharing, may be diluted or sidelined in the negotiation process.

For the United States, ensuring these agreements survive legal challenges requires recalibration. Cocreation must replace templated approaches, with explicit language affirming respect for domestic legal frameworks and decisionmaking processes. Notably, the press release for the recently signed U.S.-Senegal bilateral health agreement included such text: "This MOU does not . . . give the U.S. access to private patient data. Data protections remain governed by Senegalese law." This addition indicates that recalibration is already underway.

Regulatory compliance must be resourced within the design process and not assumed. The template language itself may require strengthening—including clearer provisions on data protection, explicit limits on the secondary use or onward sharing of health data beyond the scope of health cooperation, and more robust mechanisms for benefit sharing where data contributes to scientific or commercial innovation. A focus on speed and the number of concluded agreements should give way to a more robust instrument development process that prioritizes legitimacy—earned through transparent negotiation—even though it may take time.

African governments should learn from these early developments and exert agency, too. Kenya's response to the agreement demonstrates that African governments should be wary of sacrificing data sovereignty in favor of material gain. In Kenya, data is explicitly framed—in the Kenya Artificial Intelligence Strategy—as a strategic national asset; the strategy commits the state to safeguards that embed data sovereignty at the core of technological development. Bilateral health agreements must therefore speak from the same script, even where data access is tied to external financing. Such agreements can no longer be treated as immune to domestic accountability simply because they deliver financial or technical support. Where they involve health data or biological materials, they directly engage constitutional rights, statutory protections, and public trust.

While the United States is advancing a clear global health strategy, Kenya and other African governments' approaches to health assistance and cooperation are less clear. African governments' engagements on these agreements too often appear reactive, shaped by funding cycles rather than anchored in a clear national or regional blueprint. Articulating a coherent foreign policy position on funding—over a broader context of sovereignty, economic security, health data governance, and cooperation—would substantially reinforce African agency and negotiating authority. Finally, governments should invest in proactive public communication. Kenya illustrates the dangers of silence: When governments do not communicate clearly, they risk fostering mistrust, speculation, and litigation.

> **Kenya's response to the agreement demonstrates that African governments should be wary of sacrificing data sovereignty in favor of material gain.**

Conclusion: Data as a Strategic Asset

This new wave of U.S.-Africa health cooperation reveals a central tension in contemporary global health diplomacy: Data is no longer a technical input but a strategic asset that shapes power, value creation, and sovereignty. As African countries strengthen legal and regulatory frameworks to protect sensitive data, these domestic constraints can no longer be treated as peripheral in international health agreements.

For the United States, if the AFGHS is to function as a credible foreign policy anchor in Africa, its bilateral instruments must align with the continent's evolving legal frameworks and sovereignty assertions. Agreements that depend on access to health data must therefore incorporate clearer safeguards on data governance, benefit sharing, and regulatory compliance within partner countries. For African governments, the lesson is equally clear. If they wish to reap the financial rewards of participating in the AFGHS, they should ensure adherence to national data protections; Kenya's response should be read not as an anomaly, but as an early warning.

About the Authors

Jane Munga is a fellow in the Africa Program at the Carnegie Endowment for International Peace, where she leads research on technology policy. Her work addresses how African countries can harness digital technologies to advance inclusive and sustainable growth. Her work focuses on the nexus of digital policy, digital partnerships, and developing the foundational elements of digital development.

Rose Mosero is a tech policy expert who previously served as Kenya's deputy data commissioner and contributed to the development of the country's data protection regulatory framework and the Digital Health Act. Mosero currently serves as a regional data protection and cybersecurity expert adviser, supporting regional integration and cross-border data governance frameworks within the East African Community.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE