HHR Health and Human Rights

DREXEL UNIVERSITY Dornsife School of Public Health

FXB Center for Health & Human Rights at Harvard University

VIEWPOINT

Health Data Protection and Governance Under the Kenya–US Health Agreement

ALLAN MALECHE, SHARIFAH SEKALALA, AND TIMOTHY WAFULA

On December 4, 2025, Kenya and the United States signed a health cooperation framework aimed at "guiding collaboration to eliminate HIV, malaria, TB, and other emerging infectious diseases; strengthen Kenya's health system toward self-reliance; and advance US interests abroad, including strengthening the US–Kenya partnership."[1] This was the first bilateral agreement signed as part of the Trump administration's Make America Healthy Again campaign.[2] While the Kenya–US agreement is framed as beneficial to both governments in detecting, preventing, and responding to emerging and existing infectious disease threats, the extensive data sharing obligations raise fundamental human rights questions on data protection, privacy, consent, accountability, and state responsibility with regard to the realization of the right to health.

These serious concerns about data sharing led to the High Court of Kenya issuing conservatory orders suspending implementation of the agreement pending the hearing and determination of the case challenging it.[3] Underlying these concerns are fears that gaps in confidentiality, informed consent, and accountability in the use of health data may discourage individuals from seeking care, particularly for stigmatized conditions such as HIV and tuberculosis, and may therefore disproportionately harm the most marginalized.

Data sharing, especially around surveillance, always raises concerns that health data could be used to discriminate against marginalized groups and exclude them from having access to health care.[4] These anxieties were amplified in the COVID-19 pandemic, when digital health data were used to promote discriminatory processes against migrants, LGBTQ populations, and homeless people.[5] Digital health data also risk being securitized in a way that exceeds public health objectives. During the COVID-19 pandemic, the governments of Israel, Kenya, Mexico, and Turkey, among others, reportedly used COVID-19 data to

Allan Maleche, LLB, LLM, is an advocate of the High Court of Kenya and executive director of the Kenya Legal and Ethical Issues Network on HIV & AIDS, Nairobi, Kenya.

Sharifah Sekalala, PhD, is a professor of global health law at the University of Warwick and director of the university's Centre for Global Health Law, Coventry, United Kingdom.

Timothy Wafula, LLB, LLM, is an advocate of the High Court of Kenya and a senior program manager at the Kenya Legal and Ethical Issues Network on HIV & AIDS, Nairobi, Kenya.

Please address correspondence to Allan Maleche. Email: amaleche@kelinkenya.org.

Competing interests: None declared.

analyze private communications under the guise of contact tracing.[6]

The increased role of private actors in the collection, storage, and secondary use of big data also leads to fears around transparency, accountability, and long-term harms to vulnerable groups. Once data move into private ownership, they can be merged with other datasets for commercial purposes. It is then extremely difficult to create accountability mechanisms for misuse, especially in cases of future health harms such as insurance denials based on non-transparent risk assessments generated through large artificial intelligence health datasets.[7]

Data sharing implications of the Kenya–US agreement

Under the framework, Kenya will provide aggregated and system-level data from national digital health platforms and share programmatic and outcome data for US-supported health programs in Kenya.[8]

This agreement enables the large-scale collection, processing, and cross-border transfer of health data, raising questions about necessity, proportionality, and accountability under Kenya's constitutional and international human rights obligations.

It contains several provisions that, on their face, seek to address data protection concerns. These include commitments that data provision will comply with Kenyan law, that Kenya shall not provide individual-level or personally identifiable information "to the maximum extent practical," that the United States shall use the data solely for purposes consistent with the metrics or activities under the agreement, that the US government shall take all reasonable measures to protect the confidentiality of information shared, and that Kenya retains sole ownership of the data and all intellectual property rights.[9] The agreement also states that Kenyan law prevails where there is disagreement and requires notification of data breaches involving personally identifiable information.[10] However, the presence of formal safeguards does not, on its own, guarantee effective protection, particularly where enforcement, oversight, and remedies remain uncertain.

Although these clauses appear to align with domestic legal frameworks, including the Data Protection Act of 2019 and the Digital Health Act of 2023, closer scrutiny exposes substantial gaps that give rise to serious data protection concerns.

Risk of sharing personal identifiable health information

In Kenya, health data are classified as sensitive personal information that must be processed lawfully, fairly, and transparently; collected for specific and legitimate purposes; limited to what is necessary; kept accurate and up to date; retained only for as long as necessary; and protected from unauthorized transfer outside Kenya unless adequate safeguards or the data subject's consent are in place.[11]

The Kenya–US agreement aims to limit data sharing to aggregate-level data, which aligns with the data minimization principle under the Data Protection Act. However, the framework appears to permit broad access to Kenyan health data by the United States despite the increasing risks of re-identification, especially around genomic information and longitudinal surveillance data.

The agreement limits US use of the data to the purposes specified under the cooperation framework and expressly prohibits any use beyond those purposes, consistent with the principle of purpose limitation under the Data Protection Act. However, the mechanisms for enforcing these restrictions remain unclear. It is not evident whether Kenya has effective measures in place to verify how the United States will utilize the health data collected. Furthermore, the scope of permitted access—encompassing activities such as surveillance, analytics, reporting, and emergency response—is so broad that monitoring or verifying specific uses may be impracticable. In effect, compliance appears to rely largely on mutual trust and goodwill between the parties, raising concerns as to whether this provides sufficient protection against prohibited use.

Such risks are not abstract. Where individuals

fear that their health data may be repurposed for surveillance, profiling, or punitive state action, they may avoid testing, treatment, or engagement with public health programs. This undermines core elements of the right to health, including the accessibility and acceptability of health care services, particularly for already marginalized populations.

There are also concerns about function creep in the use of accessed health data. Disease-specific surveillance systems—particularly those relating to HIV, tuberculosis, and other stigmatized conditions—carry heightened risks of discrimination and social harm, including profiling, targeting, and further exclusion of affected populations. Considering the United States' recent positions on human rights, gender identity, and diversity, it is unclear what safeguards will be in place to ensure that such data access does not exacerbate stigma, criminalization, or structural vulnerabilities. Additionally, there is a need for clear safeguards to establish explicit firewalls between health data systems and their use for law enforcement, immigration control, and employment-related purposes.

Data ownership without control

The Digital Health Act designates health data as a strategic national asset and underscores the obligation to safeguard its privacy, confidentiality, and security in information sharing and use. While the Kenya–US agreement affirms that Kenya retains sole ownership of the data and all associated intellectual property rights in the covered data systems, the agreement appears to cede significant control over the data to the United States, potentially leaving Kenya without effective mechanisms to exercise or enforce those ownership rights. This raises concerns regarding Kenya's ability to prevent misuse, ensure timely deletion, or regulate the incorporation of the data into secondary datasets, beyond the agreed scope and duration.

In this context, data ownership without effective control risks becoming symbolic rather than substantive, weakening Kenya's ability to exercise health data sovereignty.

Conclusion

We recommend that the Office of the Data Protection Commissioner, which is the primary authority for regulating data in Kenya, play a central role in scrutiny and approval of these data sharing agreements so that it can ensure data minimization and confidentiality and so that safeguards against re-identification in aggregate form are maintained. This will involve scaling up the resources of this vital service and ensuring greater collaboration with the Ministry of Health.

Second, civil society has an important role to play in bringing together marginalized communities to participate, in enabling independent audits of compliance, and in ensuring and scrutinizing ongoing public reporting of how public health data are used and safeguarded. This may require clearer approval mechanisms for cross-border health data transfers, independent audits of compliance, and public reporting on how shared data are used and safeguarded.

Given the recognition of health data as a public good, there have been strong calls for a right to health approach to data sharing that prioritizes equitable rather than extractive practices; emphasizes the collective responsibilities of the state and private actors involved in the collection, storage, and processing of data; and ensures that all data sharing processes—including those established through bilateral agreements such as this one—uphold due process and strengthen participation and inclusion safeguards, particularly for marginalized and discriminated groups.

References

1. Government of the Republic of Kenya and Government of the United States of America, Cooperation Framework Between the Government of the Republic of Kenya and the Government of the United States of America on Health (2025), para. 1.

2. S. Lewis, "U.S. Signs Pact With Kenya Under 'America First' Global Health Plan," Reuters (December 4, 2025), https://www.reuters.com/business/healthcare-pharmaceuticals/us-signs-pact-with-kenya-under-america-first-global-health-plan-2025-12-04/.

3. G. Mosoku, "Court Suspends U.S.–Kenya Health Data

Sharing Deal," *The Star* (December 11, 2025), https://www.the-star.co.ke/news/2025-12-11-court-suspends-us-kenya-health-data-sharing-deal.

4. S. Sekalala, S. Dagron, L. Forman, and B. M. Meier, "Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance During the COVID-19 Crisis," *Health and Human Rights* 22/2 (2020).

5. Ibid.

6. Privacy International, "Knesset Committee Denies Extension of Police Access to Mobile Phone Location Data" (May 6, 2020), https://privacyinternational.org/examples/3770/knesset-committee-denies-extension-police-access-mobile-phone-location-data; Privacy International, "Kenya Tracks Mobile Phones for Quarantine Enforcement (April 9, 2020), https://privacyinternational.org/examples/3662/kenya-tracks-mobile-phones-quarantine-enforcement; Privacy International, "Mexican Telcos Grant Government Access to Cell Phone Antennas" (March 31, 2020), https://privacyinternational.org/examples/3691/mexican-telcos-grant-government-access-cell-phone-antennas; "Turkey to Use Mobile Data to Track Isolation," *Hürriyet Daily News* (April 9, 2020), https://www.hurriyetdailynews.com/turkey-to-use-mobile-data-to-track-isolation-153698.

7. Sekalala et al. (see note 4).

8. Government of the Republic of Kenya and Government of the United States of America, Cooperation Framework (see note 1).

9. Government of the Republic of Kenya and Government of the United States of America, Data Sharing Agreement Between the Government of the Republic of Kenya and the Government of the United States of America (2025), arts. 2(a), 3(a), 3(b), 3(d).

10. Ibid., arts. 3(b), 5(f).

11. Kenya Government, Data Protection Act (2019), sec. 25.