Ethics of AI in global health research

Cape Town, 29&30 November 2022

Global Forum on Bioethics in Research

Governance paper
Governance of cross-border transfer of data in Sub-Saharan Africa

Nezerith Cengiz
Centre for Medical Ethics and Law, WHO Collaborating Centre in Bioethics, Department of Medicine, Faculty of Health Sciences, Stellenbosch University, South Africa

Co-authors: Dr Dirk Brand, Prof Jerome Amir Singh, Prof Annelize McKay, Prof Keymanthri Moodley

Brief description of the context

Large research networks and collaborative projects in sub-Saharan Africa (SSA) mean that data must often be transferred or shared amongst African and international countries. SSA's most research-intensive countries are characterised by diverse data management and privacy governance frameworks. Such regional variance can impede time-sensitive data sharing and highlights the need for urgent governance reforms to facilitate effective decision-making in response to rapidly evolving public health threats. Data access, sharing and transfer between countries are crucial to effectively managing current and future health pandemics. This requires high-quality, comprehensive datasets that can inform policymaking and enhance healthcare decision-making. Data access and sharing, however, raises questions about personal privacy, the adequacy of governance mechanisms to regulate cross-border data flows, and ethical issues relating to the collection and use of personal data in the interests of public health. We explore governance considerations that ought to apply to the collection, transfer, and use of data; and provide an overview of the prevailing data-sharing governance landscape in SSA's most research-intensive countries. As a result, we identify some key limitations and gaps that impede effective data collation, sharing and analysis. A range of stakeholders such as data scientists, researchers, artificial intelligence (AI) coders, and government decision-makers may benefit from and find this paper useful. The issues explored here are of universal concern and therefore of relevance to the African context as well as a broader international audience.

Commentary

The sharing/transfer of data between countries and national institutions in SSA significantly strengthens research capacity.[1;2] However, concerns regarding the cross-border flow of data and privacy protection have been raised. Africa lacks the capacity and resources to build, maintain, and analyse large data sources and datasets required by AI systems; consequently hindering the continents' ability to make informed, evidence-based decisions in healthcare or policy development to describe related challenges.[2] Data protection legislation in SSA does not, often, adequately address the lawful use of data in the development of AI tools although it is required to guide its ethical use in healthcare and offer guidance to software developers and other stakeholders.[1;3] Since large datasets are required in the development of AI tools in healthcare, concerns about privacy, accountability, and transparency among others are raised as its misuse could adversely impact individual data subjects and/or society.[1;2;3;4] Accordingly, data ethics plays a vital role in developing AI applications and evaluating large datasets and related activities (collection, analysis, sharing/transfer, and use).

Table 1 categorises the rigour of national data protection laws concerning the cross-border transfer of personal data.[1;5] Table 1 is not aimed at providing a strict overall categorisation of

various data protection laws, but rather, is focused on the scope of legal protection afforded to data subjects regarding the cross-border transfer of their personal data. Countries with stringent rules require notification of, or approval by, a relevant data protection authority, and/or special conditions (such as proof of appropriate safeguards concerning the protection and security of personal data), as well as consent from the data subject.

South Africa and Kenya count among the countries that could be described as providing stringent data export protection to data subjects. For example, Kenya's Data Protection Act of 2019 complies with the European Union (EU) legal standards, which are generally regarded as being stringent in nature. For data to be transferred out of Kenya, the data processor must verify to the data commissioner that the third-party recipient's jurisdiction is bound by appropriate safeguards for the security and protection of the data. It is also important that the data transfer be purposeful, such as necessary for the conclusion or performance of a contract, a legal claim, and public or data subjects' interests. In addition, consent from the data subject is also required for cross-border data transfers.[1;5]

Countries falling in the moderate category allow for more than one possible legal ground to permit data export, such as consent of the data subject, but do not require notification or approval by the data protection authority. Nigeria counts amongst countries providing moderate data export protection to data subjects as the country's data protection law does not require third-party recipients of data to be bound by adequate data protection law, agreements, or corporate rules if the data subject provides consent after being informed of possible risks of inadequate data protection or if the transfer meets a certain exception. One example of such an exception is the public's or data subject's interest. Beyond obtaining consent from data subjects for data transfers, the Nigeria Data Protection Regulation 2019 requires the National Information Technology Development Agency (NITDA) or Honourable Attorney General of the Federation (HAGF) to ensure that the third-party recipients of the transferred data have adequate data protection standards in place.[1;5]

Ghana's data protection legislation does not contain any provisions pertaining to the cross-border transfer of personal information and could thus be described as providing inadequate protection to data subjects in relation to the export of their personal data.[1;6]

The diverse legal landscape governing data sharing in sub-Saharan Africa – including the stringency of data export provisions – highlights that cross-border data transfers will have to be evaluated on a case-by-case basis as there is no uniform law across the continent akin to the General Data Protection Regulation (GDPR) (2018), which constitutes a common legal framework for all EU Member States. Although the AU Commission is developing a data policy framework for Africa to harness digital technologies and innovation in an attempt to bridge the digital divide, this process is ongoing and will take time to implement.[1;7]

Table 1: *Sub-Saharan Africa country rankings by research output ("Public Health, Environment, and Occupational Health").*[1;8]

Rank and country	Legal Requirements	Legislation	Data export protection classification
South Africa	A responsible party may only transfer personal data outside South Africa if the recipient is subject to a law, binding corporate rules or the binding agreement that provide adequate protection. Or the data subject consents to the transfer; or The transfer is necessary for the terms of the provisions of the Act.	Sec. 72 of the Protection of Personal Information Act, 4 of 2013 (South Africa)	Strict
Nigeria	Cross-border transfer of personal data is subject to authorisation by the Attorney General or the National Information Technology Development Agency (NITDA) based on an adequate level of protection. In the absence of authorisation by the Attorney General or the Agency, personal data transfer may only take place if the data subject gave consent, or the data transfer is necessary in terms of the Regulation.	Reg. 2.11 and 2.12 of the Nigeria Data Protection Regulation, 2019.	Moderate
Kenya	Only allowed if there is proof of adequate data protection safeguards or consent from the data subject. Data controller or data processor must provide proof to Data Commissioner on appropriate safeguards. The data transfer must be necessary in terms of the Act.	Sec. 25(h) 48 of the Data Protection Act, No. 24 of 2019 (Kenya)	Strict
Ethiopia	Cross-border data transfer may only take place subject to an adequate level of data protection in the recipient country. Data controller or data processor must provide proof to Data Protection Commission of appropriate level of protection, or the data subject has given consent to the proposed transfer, or the transfer is necessary, or the transfer is made from a register and intended to provide information to the public.	Sec. 27-30 of the Draft Proclamation to Provide for Personal Data Protection, 2021 (Ethiopia)	Strict
Uganda	Data processors or data controllers must ensure that there are adequate measures in place for the protection of personal data, or the data subject must provide consent.	Sec. 19 of the Data Protection and Privacy Act, 2019 (Uganda)	Strict

Conclusion and recommendations

Given the lack of data protection legislation in SSA, we aim to provide guidance on ethical data sharing. Harmonised data sources and their integration into national health information systems will create a comprehensive dataset. A holistic approach to data management should underpin evidence-based decision-making. To facilitate cross-border data transfers involving personal data, standard contractual provisions and templates for cross-border data transfers should be developed by data protection authorities in Africa. Doing so will facilitate not just scientific cooperation between countries, but also facilitate an integrated cross-border approach to the management of future pandemics. SSA countries should aim to strengthen their digital infrastructure for capturing and storing data to aid in building appropriate analytical capacity. To enhance both the use of and access to data in the context of AI, principles of transparency, fairness, and accountability would strongly aid with the establishment of a reliable and accessible digital ecosystem in SSA.

References

1. Brand, D., Singh, J. A., McKay, A. G. N., Cengiz, N., & Moodley, K. (2022). Data sharing governance in sub-Saharan Africa during public health emergencies: Gaps and guidance. South African Journal of Science, 118(11/12). https://doi.org/10.17159/sajs.2022/13892
2. The World Health Organisation. Ethics and governance of artificial intelligence for health. 2021 June 28 [cited 2022 June 15]. Available from: https://www.who.int/publications/i/item/9789240029200
3. Owoyemi A, Owoyemi J, Osiyemi A, Boyd A. Artificial Intelligence for Healthcare in Africa. Front Digit Health. 2020 Jul 7;2:6. doi: 10.3389/fdgth.2020.00006. PMID: 34713019; PMCID: PMC8521850.
4. Abebe R, Aruleba K, Birhane A, Kingsley S, Obaido G, Remy S, et al. Narratives and Counternarratives on Data Sharing in Africa. In: 2021 FAccT ACM Conference on Fairness, Accountability, and Transparency. ACM FAccT; 2021. p. 329–41.
5. Suominen K, Vambell E. Alliance for E-Trade Development: Toward an African Data Transfer Regime to Enable MSMEs' Cross-border Ecommerce [Internet]. 2021 Sep [cited 2022 June 15]. Available from: https://www.allianceforetradedevelopment.org/_files/ugd/478c1a_72021e35a826441db0723642a79e65e5.pdf
6. The Parliament of the Republic of Ghana. Data Protection Act, 2012. Data Protection Act, 2012, 843 Republic of Ghana; Oct 16, 2012.
7. Africa Union. The digital transformation strategy for Africa (2020-2030) [Internet]. Addis Ababa; 2021 Aug [cited 2022 June 15]. Available from: https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf
8. Scimago Journal & Country Rank. Country Rankings: Public Health, Environment, and Occupational Health [Internet]. Scimago Journal & Country Rank. 2022 [cited 2022 Aug 23]. Available from: https://www.scimagojr.com/countryrank.php?region=Africa&category=2739 from: https://www.allianceforetradedevelopment.org/_files/ugd/478c1a_72021e35a826441db0723642a79e65e5.pdf

This paper was prepared for GFBR 2022. Further details on the meeting are available at www.gfbr.global.