AUTHORS:
Donrich Thaldar[1,2]
Lukman Abdulrauf[1,3,4]
Paul Ogendi[1,5]
Amy Gooden[1]
Dusty-Lee Donnelly[1]
Beverley Townsend[1,6]

AFFILIATIONS:
[1]School of Law, University of KwaZulu-Natal, Durban, South Africa
[2]Petrie-Flom Center for Health Policy, Biotechnology, and Bioethics, Harvard Law School, Cambridge, Massachusetts, USA
[3]Department of Public Law, Faculty of Law, University of Ilorin, Ilorin, Nigeria
[4]Center for Advanced Study in the Behavioral Sciences (CASBS), Stanford University, Stanford, California, USA
[5]Faculty of Law, University of Nairobi, Nairobi, Kenya
[6]York Law School, University of York, York, UK

CORRESPONDENCE TO:
Donrich Thaldar

EMAIL:
ThaldarD@ukzn.ac.za

HOW TO CITE:
Thaldar D, Abdulrauf L, Ogendi P, Gooden A, Donnelly D-L, Townsend B. Response to Brand et al. (2022) 'Data sharing governance in sub-Saharan Africa during public health emergencies'. S Afr J Sci. 2023;119(11/12), Art. #15722. https://doi.org/10.17159/sajs.2023/15722

ARTICLE INCLUDES:
☐ Peer review
☐ Supplementary material

KEYWORDS:
data, data sharing, governance, sub-Saharan Africa, public health emergencies

FUNDING:
US National Institutes of Health (U01MH127690)

PUBLISHED:
29 November 2023

Response to Brand et al. (2022) 'Data sharing governance in sub-Saharan Africa during public health emergencies'

Significance:

Various aspects of Brand et al.'s (S Afr J Sci. 2022;118(11/12), Art. #13892) overview of Africa's data protection legislation require clarification. Most pertinently, we provide the following clarifications:

- Ghanaian law does provide for cross-border data transfers; statements about the law being "inadequate" ought to be well substantiated.
- Nigerian law provides for adequacy decisions – not authorisations – in respect of cross-border data transfers.
- Kenyan law provides for an important exception relevant to public health emergencies.
- South African law currently requires, amongst others, prior authorisation from the Information Regulator for cross-border transfers of health data.
- South Africa does not yet have a code of conduct for research.

Introduction

We start with some background. In 2021, Steytler and Thaldar published a review of recommendations for legal reform in South Africa relating to, inter alia, data sharing during public health emergencies.[1] These recommendations include, in respect of health data: (a) the creation of an African Data Corridor, (b) the adoption of open access research data, and (c) the development of data trusts, as suggested by the Organisation for Economic Co-operation and Development (OECD), and in respect of geospatial data used for health research: (d) an amendment to the *Space Affairs Act 84 of 1993*.[1] Recommendations (a) to (c) were based on the work of Townsend[2], and (d) on the work of Botes[3].

In their recent article in this journal, Brand et al.[4] add their voices to the discourse on improving data sharing governance during public health emergencies. We agree with the authors' recommendations, most pertinently the development of standard contractual clauses and data transfer agreement templates. These measures would indeed facilitate cross-border data transfer, as has been suggested in the South African (and African) context by Townsend[2].

However, we suggest that multiple aspects of Brand et al.'s overview of Africa's data protection legislation require clarification. In this article, we highlight the most salient of these aspects. Also, given the focus of Brand et al. on sub-Saharan Africa, we suggest that the authors' arguments could benefit significantly from being positioned within the relevant African Union (AU) policy framework.

Legal aspects requiring clarification

Ghanaian law does provide for cross-border data transfers; statements about the law being "inadequate" ought to be well substantiated

Brand et al.[4] state as follows regarding Ghana:

> *Ghana's data protection legislation does not contain any provisions pertaining to 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.*

This statement requires some analysis. The Ghanaian *Data Protection Act, 2012 (Act 843)* (DPA) defines the *processing* of information as including the "disclosure of the information or data by transmission, dissemination or other means available" (section 96 of the Ghanaian DPA), which would include the cross-border transfer of data out of Ghana. As such, we suggest that Brand et al.'s statement that Ghana's data protection legislation "does not contain any provisions pertaining to cross-border transfer"[4] be clarified. First, all the provisions of the Ghanaian DPA that govern the *processing* of information would apply to the cross-border transfer of data out of Ghana. These include, inter alia, compliance with Ghanaian law by foreign data processors (section 30(4) of the Ghanaian DPA). Moreover, the Ghanaian DPA provides for an extra layer of protection for sensitive data, which includes health data. Sensitive data may only be transferred outside of Ghana if: (1) there is consent, or (2) the transfer is necessary for medical purposes, which are defined to include 'health research' (section 37(6) and (7) of the Ghanaian DPA).

Brand et al. do not explain why, in their view, these protections afforded by the Ghanaian DPA are "inadequate"[4]. This is a strong claim, and clearly requires more substantiation. Can such substantiation be that Ghana is not included in other jurisdictions' adequacy lists? While the European Commission's adequacy list is well known[5], one should keep in mind that it does not include a single African country, and therefore does not provide grounds to single out Ghana

as being inadequate, as Brand et al. do. By contrast, Nigeria, Africa's largest economy[6], includes Ghana in its adequacy list (the South African Information Regulator has not yet issued a South African adequacy list). We suggest that Brand et al.'s statement that the Ghanaian DPA – in contrast with, for example, the South African, Nigerian, or Kenyan data protection statutes – is "inadequate" in respect of the protection that it affords to data subjects regarding the cross-border transfer of their personal data, clearly requires more substantiation.

Nigerian law provides for adequacy decisions – not authorisations – in respect of cross-border data transfers

In Table 1 of their article, with regard to Nigeria, Brand et al. state that "cross-border transfer of personal data is subject to *authorisation* by the Attorney General or National Information Technology Development Agency (NITDA) based on an adequate level of protection"[4] (own emphasis). In our reading, this is not the case. To clarify, the role of NITDA and the Honourable Attorney General of the Federation is to make decisions regarding adequacy (regulation 2.11 of the *Nigeria Data Protection Regulation, 2019* (NDPR)), which is not the same as providing authorisation. These institutions have indeed developed a 'whitelist' of countries that are deemed adequate.[7] This means that any person seeking to transfer health data out of Nigeria to a whitelisted country can do so freely. By contrast, if a person seeks to transfer health data out of Nigeria to a country that is not whitelisted, then they must rely on any of the legal conditions, such as consent and public interest (regulation 2.12 of the NDPR). The recently signed *Data Protection Act 2023* also maintains a similar position to the NDPR, namely that the Nigerian Data Protection Commission is *only* to make decisions regarding adequacy and not to grant authorisations (section 42(4) of the Nigerian Data Protection Act). Therefore, it is clear that Nigerian law does not require authorisation for cross-border data transfers – whether it is to a whitelisted country or not.

Kenyan law provides for an important exception relevant to public health emergencies

Brand et al. suggest that Kenya is amongst the countries that could be described as providing "stringent" data export protection to data subjects.[4] The authors define "stringent" protection as rules that[4]:

> *require notification of, or approval by, a relevant data protection authority, and/or special conditions (such as proof of appropriate safeguards with respect to the protection and security of personal data), as well as consent from the data subject.*

Although this description might apply to the *general* rules of Kenyan data protection law, we suggest that Brand et al. do not take adequate cognisance of an important exception to these rules in the context of public health emergencies. In terms of the Kenyan *Data Protection (General) Regulations, 2021*, if there is a "permitted health situation" or a "permitted general situation" that necessitates the cross-border sharing of health data, the legal requirements for prior authorisation from the Kenyan Data Commissioner and consent from data subjects are both waived. Accordingly, in this way, Kenyan law is designed to significantly relax its data protection rules in situations such as public health emergencies.

For the sake of comprehensiveness, it should be mentioned that if health data are anonymised in terms of the Kenyan *Data Protection Act 24 of 2019*, this statute and its cross-border data transfer requirements would not apply to such data. (Note that Kenyan law uses the term *anonymise*. The corresponding – but not equivalent – term in South African law is *de-identify*.) However, we recognise that such anonymisation may be impossible or undesirable from a research perspective. In such cases, reliance can be placed on the exception discussed above.

South African law currently requires, amongst others, prior authorisation from the Information Regulator for cross-border transfers of health data

Brand et al.'s description of South Africa's legal requirements for the cross-border sharing of personal information, as presented in Table 1 of their article, refers only to section 72 of the *Protection of Personal Information Act 4 of 2013* (POPIA).[4] However, if the relevant personal information is *health* information, it would additionally qualify as *special* personal information, and hence *also* trigger section 57(1)(*d*) of POPIA. This provision requires prior authorisation from the Information Regulator for transfers to a third party in a foreign country that does not provide an adequate level of data protection – except if a code of conduct has come into force for the relevant sector (section 57(3) of POPIA). Given that: (a) the Information Regulator has not yet issued a list of foreign countries that it deems to provide an adequate level of data protection, and (b) as there is not yet a code of conduct in force for research, section 57(1)(*d*) of POPIA would apply, and should, we suggest, have been included in Table 1 of Brand et al.'s article. (The issue of a code of conduct is addressed more fully below.)

Of course, similar to the case with Kenyan law discussed above, if health data are de-identified in terms of POPIA, POPIA would cease to apply, and there would be no legal requirement for the cross-border transfer of such data. Note, however, that de-identification in terms of POPIA requires that there must be *no reasonably foreseeable method* to re-identify the data (section 1 of POPIA). Such de-identification of health data may not always be possible or desirable from a research perspective. If health data are not de-identified, as contemplated in POPIA, any person intending to transfer such health data to a foreign country would need to comply with both sections 72 *and* section 57(1)(*d*) of POPIA.

South Africa does not yet have a code of conduct for research

Brand et al. state that the Academy of Science of South Africa (ASSAf) "has developed a privacy Code of Conduct for Research"[4], and then proceed to refer to it as "The Code"[4]. For clarity, as of the date of writing this response, the *proposed* Code of Conduct for Research that was developed by ASSAf has been submitted to the Information Regulator, but is yet to be approved.[8] The Information Regulator may still request amendments. Only if, and when, the Information Regulator eventually approves the *proposed* Code of Conduct for Research will it have the legal status of a code of conduct.

Developments in the African policy sphere

An important step towards data protection integration and collaboration within Africa was taken with the endorsement of the AU Data Policy Framework by the AU Executive Council in February 2022.[9] The AU Data Policy Framework makes detailed recommendations to guide African countries through the formulation of policy in their domestic context, as well as recommendations to strengthen cooperation among countries and promote intra-Africa flows of data.[9] However, Brand et al. seem to be under the impression that the AU Data Policy Framework is still under development. (The authors state that: "[T]he AU Commission is developing a data policy framework for Africa…."[4]) Consequently, Brand et al. present their recommendations without reference to the AU Data Policy Framework, and without acknowledgment that most of their recommendations have already been covered by the comprehensive recommendations made in the AU Data Policy Framework – a document that precedes the initial submission date of the authors' article by three months. Brand et al.'s work could have benefitted significantly from being positioned within the AU Data Policy Framework.

It is interesting to note the way in which the AU Data Policy Framework classifies cross-border data regimes. While Brand et al. describe a "stringent", or a "strict", and a "moderate" categorisation of cross-border data governance regimes[4], in contradistinction, the AU Data Policy Framework offers three stylised approaches to cross-border data governance, namely: (a) an 'open transfer', (b) a 'conditional transfer', and (c) a 'limited transfer' model.[9] This approach is drawn from the recent work of Ferracane and Van der Marel[10,11]. In a 'limited transfer' model, cross-border data flows are conditional upon governmental approval and localisation requirements for domestic storage or processing of data. Examples provided by the AU Data Policy Framework are that of China and Russia.[9] At the other end of the spectrum, an 'open transfer' model has relatively low a priori mandatory approval requirements and relies on voluntary standards. Between these two

models is the 'conditional transfer' model, which provides guidelines and mandatory regulatory safeguards which, once met, allow for the free transfer of data. Accordingly, it is our contention that South Africa would count as a 'conditional transfer' regime: that is, it is consensus-based, with established regulatory data safeguards and overarching regulatory guidance from data protection authorities or international agreements – not unlike the European Union's (EU) *General Data Protection Regulation, 2018* (GDPR) – rather than that of the stricter, 'limited transfer' model which is based on "strong national security and public data control imperatives"[9].

Concluding notes

The topic of cross-border data sharing – especially the sharing of *health* data, and particularly during public health *emergencies* – should be a public policy development *priority*. Academic discourse can – and should – contribute constructively to this important process. It is in this spirit that we offer our response to Brand et al., and we invite the authors to engage with the entirety of our research group's past, present, and future research. Only through such a dialectic process can the academic discourse be clarified and improved.

Acknowledgements

We are grateful to Simisola Akintola and Peter Munyi for their valuable comments on drafts of this manuscript. All remaining errors are the authors' alone. We acknowledge the support of the US National Institute of Mental Health and the US National Institutes of Health (award number U01MH127690). The content of this article is solely our responsibility and does not necessarily represent the official views of the US National Institute of Mental Health or the US National Institutes of Health.

Competing interests

We have no competing interests to declare.

References

1. Steytler M, Thaldar DW. Public health emergency preparedness and response in South Africa: A review of recommendations for legal reform relating to data and biological sample sharing. S Afr J Bioethics Law. 2021;14(3):101–106. https://doi.org/10.7196/SAJBL.2021.v14i3.772
2. Townsend B. The lawful sharing of health research data in South Africa and beyond. Inf Commun Technol Law. 2021;1–18. https://doi.org/10.1080/13600834.2021.1918905
3. Botes M. The use of geospatial surveillance data for public-health emergency and disaster management in South Africa: A review with legal recommendations. Tydskr Suid-Afr Reg. 2021;3:474–503. https://doi.org/10.47348/TSAR/2021/i3a4
4. Brand D, Singh JA, Nienaber McKay AG, Cengiz N, Moodley K. Data sharing governance in sub-Saharan Africa during public health emergencies: Gaps and guidance. S Afr J Sci. 2022;118(11/12), Art. #13892. https://doi.org/10.17159/sajs.2022/13892
5. European Commission. Adequacy decisions [webpage on the Internet]. No date. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
6. World Bank. GDP (current US$) [data set on the Internet]. No date. Available from: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD
7. Nigerian National Information Technology Development Agency (NITDA). Nigeria Data Protection Regulation 2019: Implementation framework. NITDA; 2020. Available from: https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf
8. Academy of Science of South Africa (ASSAf). POPIA Code of Conduct for Research. Pretoria: ASSAf; 2023. Available from: https://www.assaf.org.za/wp-content/uploads/2023/04/ASSAf-POPIA-Code-of-Conduct-for-Research.pdf
9. African Union (AU). AU Data Policy Framework. Addis Ababa: AU; 2022. Available from: https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf
10. Ferracane MF, Van der Marel E. Regulating personal data: Data models and digital services trade. Policy Research Working Papers. 2021. https://doi.org/10.1596/1813-9450-9596
11. Van der Marel E, Ferracane MF. Regulating personal data: Linking different models to digital services trade. CEPR; 2021. Available from: https://cepr.org/voxeu/columns/regulating-personal-data-linking-different-models-digital-services-trade