AUTHORS:
Dirk Brand[1]
Jerome A. Singh[2]
Annelize G. Nienaber McKay[3,4]
Nezerith Cengiz[5]
Keymanthri Moodley[5]

AFFILIATIONS:
[1]School of Public Leadership, Stellenbosch University, Stellenbosch, South Africa
[2]School of Law, University of KwaZulu-Natal, Durban, South Africa
[3]Division of Law, Abertay University, Dundee, Scotland, United Kingdom
[4]Department of Public Law, University of Pretoria, Pretoria, South Africa
[5]Centre for Medical Ethics and Law, Faculty of Medicine and Health Sciences, Stellenbosch University, Cape Town, South Africa

CORRESPONDENCE TO:
Nezerith Cengiz

EMAIL:
ncengiz@sun.ac.za

HOW TO CITE:
Brand D, Singh JA, Nienaber McKay AG, Cengiz N, Moodley K. A response to Thaldar et al. (2023): Data sharing governance in sub-Saharan Africa during public health emergencies. S Afr J Sci. 2023;119(11/12), Art. #16896. https://doi.org/10.17159/sajs.2023/16896

ARTICLE INCLUDES:
☐ Peer review
☐ Supplementary material

KEYWORDS:
legal, data sharing, public health, sub-Saharan Africa

FUNDING:
US National Institutes of Health (1U01MH127704-01)

PUBLISHED:
29 November 2023

A response to Thaldar et al. (2023): Data sharing governance in sub-Saharan Africa during public health emergencies

Significance:

We elucidate the misinterpretations raised by Thaldar et al. (S Afr J Sci. 2023;119(11/12), Art. #15722) on our previous publication in which we outlined the data sharing governance landscape in selected African countries.

We thank the SAJS for affording us the opportunity to respond to a commentary[1] on our article[2]. We will focus on the principal points as raised by Thaldar et al.[1]:

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

Section 18(2) of Ghana's *Data Protection Act of 2012* (GDPA) contains no specific provisions on international transfer of data. The mere stipulation in this section that where a foreign data subject's personal data are sent to Ghana for processing, such processing should occur in accordance with the data protection legislation of the foreign jurisdiction, does not determine international data transfer requirements for data subjects in Ghana. Further, the GDPA does not specify data transfer governance prerequisites between Ghana and foreign jurisdictions. This compares unfavourably with legislation of jurisdictions such as South Africa, which explicitly governs the transfer of personal information outside the country (Section 27).[3] We affirm our position: the GDPA offers inadequate protection to its data subjects in relation to data transfers to foreign jurisdictions.

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

At the time at which our manuscript[2] was submitted for publication (2022), Nigeria's Data Protection Regulation (DPR) of 2019 governed international data transfers in the country[4]. In 2023, the *Data Protection Act* was approved and promulgated in Nigeria, which repealed the Data Protection Regulation. In terms of the erstwhile DPR, specifically Reg. 2.11, international data transfer had to take place *under the supervision* of the Attorney General of Nigeria and *the National Information Technology Development Agency (NITDA)* had to determine whether the foreign country provided an adequate level of protection[4] (words italicised for emphasis). Authorisation for international data transfer was provided by way of a decision by NITDA.

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

The Kenyan *Data Protection Act* is clear that public interest, which includes a public health emergency, could be a legitimate basis for the lawful transfer of personal data to another country (sec. 48 (c) (iii)).[5] Furthermore, the Kenyan *Data Protection Regulations, 2021*, provide strict rules for the international transfer of data that include "adequate data protection safeguards" as an important basis for allowing the transfer.[5] The fact that provision is made for exemptions in very specific situations, such as a public health emergency, does not weaken the legislative framework. On the contrary, the overall approach of the Kenyan legislature is to have a detailed strict regulatory framework which includes allowing for special cases such as public health emergencies.

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

Section 57 of the *Protection of Personal Information Act 4 of 2013* (POPIA) specifies that the responsible party must obtain prior authorisation from the Regulator, in terms of section 58, prior to any processing – if that responsible party plans to transfer special personal information (including health information of a data subject) to a third party in *a foreign country that does not provide an adequate level of protection for the processing of personal information*, as referred to in section 72[3] (words italicised for emphasis). No such prior authorisation from the Regulator is required if the foreign country is deemed to provide an "adequate level of protection". More significantly, sections 57 and 58 are not applicable if a code of conduct has been issued and has come into force in terms of Chapter 7 in a specific sector or sectors of society.

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

ASSAf refers to its draft "Code of Conduct for Research" as "the Code"[6,7]. Reference to "the Code" in the manuscript is intended to be interpreted in this context.

Acknowledgements

We acknowledge support from the US National Institutes of Health (1U01MH127704-01).

Competing interests

We have no competing interests to declare.

References

1. 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
2. Brand D, Singh JA, McKay AGN, 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. #13982. https://doi.org/10.17159/sajs.2022/13892
3. Republic of South Africa. Protection of Personal Information Act. Act no 4 of 2013.
4. Nigerian National Information Technology Development Agency (NITDA). Nigeria Data Protection Regulation 2019 [document on the Internet]. c2020 [cited 2023 Aug 10]. Available from: https://www.dataguidance.com/sites/default/files/nigeriadataprotectionregulation11.pdf
5. Republic of Kenya. Data Protection Act, No. 24 of 2019. Kenya Gazette Supplement No.181. Available from: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
6. Adams R, Adeleke F, Anderson D, Bawa A, Branson N, Christoffels A, et al. Popia code of conduct for Research (with corrigendum). S Afr J Sci. 2021;117(5/6), Art. #10933. https://doi.org/10.17159/sajs.2021/10933
7. Academy of Science of South Africa (ASSAf). Popia code of conduct for research [document on the Internet]. c2023 [cited 2023 Aug 10]. Available from: https://www.assaf.org.za/wp-content/uploads/2023/04/ASSAf-POPIA-Code-of-Conduct-for-Research.pdf