Quest Journals
Journal of Research in Humanities and Social Science
Volume 12 ~ Issue 11 (2024) pp: 176-182
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

Protecting Digital Health Data: A Human Rights Approach

Shem OgangaNyang'au*

Abstract
For a long time, it had been assumed that frauds targeted mainly those digital databases with financial records, however, the recent spike of unauthorised access to digital health data indicates a shift which has been attributed to the insufficient data protection standards for health records stored digitally.
While the digitalisation of healthcare offers unprecedented opportunities for efficiency and innovation, it also exposes vulnerable aspects of sensitive personal data and infrastructure security. The vulnerability is exacerbated by the lack of proper mechanisms in private institutions and limited State auditing capabilities, resulting in an alarming surge in data attacks. Shockingly, due to concerns that their reputation may be jeopardised, many of these institutions choose not to report such incidents.
While the Global North has made great strides in protecting digital health data, the Global South still lags; even though many States have made huge technological shifts, significant progress has not been achieved in health data protection.
This paper illustrates the dire consequences of cyberattacks on health data. Such attacks not only compromise privacy but also disrupt critical services, putting the right to health.
By shedding light on these issues, this paper underscores the urgent need for enhanced data protection measures, improved cybersecurity protocols, and increased awareness of the collection and handling of health data. It advocates for a proactive approach to safeguarding digital privacy, ultimately ensuring unimpeded access to quality healthcare, which are essential components of a thriving society in the digital age.

Keywords: *privacy, personal data, health, digital infrastructure attacks*

***R**eceived 11 Nov., 2024; **R**evised 22 Nov., 2024; **A**ccepted 24 Nov., 2024 © The author(s) 2024.*
P**ublished with open access at **www.questjournas.org

I. Introduction

1.1. Background

The integration of the Internet of Things, Smart Devices, Information Systems, and Cloud Services in the service sector especially in the health sector has led to a massive digital transformation.[1] It also incorporates a wide range of modern technologies including artificial intelligence and machine learning.[2] While the digitalisation of these facilities is no mean feat, the online integration between several entities makes these systems vulnerable to security violations and data breaches.[3] These breaches do not just affect service provision but by accessing the sensitive data of clients in these sectors, they pose a grave danger to their personal life.[4]

* PhD research scholar, Faculty of Law, University of Delhi.

[1]SehAdilHussain, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan, "Healthcare Data Breaches: Insights and Implications", *Healthcare*, vol. 8(2020), pp. 133-151 at p.133.

[2]Popov Vladimir V., Elena V. Kudryavtseva, Nirmal Kumar Katiyar, Andrei Shishkin, Stepan I. Stepanov, and Saurav Goel, "Industry 4.0 and Digitalisation in Healthcare", *Materials*, vol.15 (2022), pp. 2140-2151 at p.2140.

[3]Muktiarni M., I. Widiaty, A. G. Abdullah, A. Ana, and C. Yulia, "Digitalisation Trend in Education During Industry 4.0." *Journal of Physics: Conference Series*. Vol. 1402. No. 7. IOP Publishing, (2019), pp. 1-7 at p .4.

[4]Hussain, *note 2.*

1.2. Pathways for Health Data Breach

Smartphones and other smart devices have been cited as one of the means by which unauthorised persons easily access the institutional digital infrastructure thereby exposing sensitive data such as personal medical history to theft or disclosure.[5] On the other hand, electronic mail and network servers have been identified as prime targets for malware, ransomware, or phishing attacks.[6]

Advancements in healthcare have led to the incorporation of not only digital infrastructure and the Internet of Medical Things but also to the invention of smart medical devices such as infusion pumps and pacemakers which are of great resource in supporting patients to lead quality lives. It should be noted that these devices rely on computer software and artificial intelligence to function and most of them are wireless therefore are linked to a central digital network. This wireless connection makes them vulnerable to hackers, viruses and other malware. Cyber security experts have established that medical devices are not advanced in cyber protection hence they are soft spots for cyber threats.[7]

As medical devices are becoming more connected to each other, hospital networks are now more connected to patients most of whose smartphones are connected to the hospital internet network thereby raising threats of cyber-attacks.[8] It is estimated that 1 out of 4 medical devices is now connected to the central infrastructure of the hospital. In one visit, a person can encounter at least 10 medical devices- this connectedness has become a major attraction for hackers who seek to target medical devices with the intention of unauthorised access to health data.[9]

1.3. Incidences of Digital Health Data Breaches

There are numerous instances where a breach of health data causes grave consequences for instance; at the University of Vermont Medical Center in the United States of America, an employee whose homeowners' association email had been hacked, opened the message through the institution's electronic gadget thereby making the ransomware spread throughout its digital network to the extent of causing electronic medical devices in the facility to malfunction at the height of Covid-19 in 2020.This brought the hospital to a halt since not even lifesaving services such as surgeries and critical patient care could function.[10]

Ransomware attacks on health facilities and institutions of learning are not just limited to the developed world, some developing countries such as India and Kenya have had quite a share of health data breaches and these malicious acts are on the rise in the Global South. For instance, the digital system of a private medical facility in Mysuru, India was attacked in November 2021. The hackers infiltrated the main financial server of the hospital and thereafter successfully gained access to the financial data and personal data of the patients including medical history. They thereafter encrypted the acquired data hence preventing the hospital staff from accessing it. This crippled the services of the hospital since the data encrypted was required to be used by the staff to serve the patients.[11]

Increased cyber-attacks on health data indicate that institutions possessing such information especially medical facilities and learning facilities are soft targets for perpetrators who intend to steal information, compromise data, divert money and build botnets. In other cases, they are used to spy, infiltrate systems and destroy key infrastructure used in hospitals and response institutions. Research has shown that the healthcare sector was the most targeted by ransomware, with attacks against hospitals increasing by 36 per cent in Europe, the Middle East and Africa and 33 per cent in Asia Pacific countries. Concern has been raised that amidst the

[5]Hussain, *note 2,* p.134.

[6]Hussain, *note 2*,p.144.

[7]Gollakota S., Hassanieh H., Ransford B., Katabi, D. and Fu K., "They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices. *Proceedings of the ACM SIGCOMM 2011 conference* (2011), pp. 2-13 at p.2.

[8] Generally, see; Ransford, B., Kramer, D. B., Foo Kune, D., Auto de Medeiros, J., Yan, C., Xu, W., & Fu, K.," Cybersecurity and Medical Devices: A Practical Guide for Cardiac Electrophysiologists", *Pacing and Clinical Electrophysiology*, vol. 40(2017), pp. 913-917.

[9]Jensen R.D., Copeland S., Domas S., Hampton R., Hoyme K., Jump M., Rekik I., Schwartz S. and Vasserman, E., "A Roundtable Discussion: Thawing Out Healthcare Technology's 'Special Snowflake' Cybersecurity Challenges." *Biomedical Instrumentation & Technology*, vol.51(2017), pp.10-16.

[10] Jenni Bergal, "Ransomware Attacks on Hospitals Put Patients at Risk," Stateline, 2022. Obtained from <https://stateline.org/2022/05/18/ransomware-attacks-on-hospitals-put-patients-at-risk> on 23/06/2022.

[11] Karthik KK, "Cybercriminals Hack Server of Mysuru Hospital, Demand Ransom in Bitcoin to Release Data", *The Indian Express*, 2021. Obtained on 23/06/2022 from: <https://www.newindianexpress.com/states/karnataka/2021/dec/01/cybercriminals-hack-server-of-mysuru-hospital-demand-ransom-in-bitcoin-to-release-data-2390500.html>

increased cyber-attacks, private entities have been hesitant to report such data breaches for fear of reprisal and damage to their reputation.[12]

1.4. Warnings on Increasing Cyber-Attacks in the Health Sector

Several state agencies have issued warnings on the imminent cyber-attacks targeting the digital infrastructure of institutions such as those in the health sector.[13] For instance, in April 2022 the American Department of Health and Human Services cautioned medical facilities to prepare for increased cyber-attacks by strengthening defences for their digital infrastructure so as to repel ransomware attacks that were on the rise in the sector. Most of these attacks have been attributed to the Hive ransomware group which has been known to be operational since June of 2021 but within such a short period has caused immeasurable damage to digital health infrastructure in facilities possessing health data.[14]

II. Quantifying Health Data Breach

Records indicate a significant spike inunauthorised access to digital health records following the digitalisation of personal medical records. It is estimated that from 2005 to 2019, at least 249.09 million people were affected by health data breaches. Pointing to the exponential rise in healthcare data breaches in the past decade, IBM established that in a 2019 survey of 86 countries, the average cost of a data breach amounted to a whopping $3.92 million, while a healthcare industry breach could cost around $6.45 million.[15]

In 2015 alone, 67% of identity breaches in the United States of America occurred in the healthcare sector. One of the reasons for the increased health data breach is the fact that it contains more sensitive data that can cause maximum harm to the data subject. For instance, unlike credit card information whose use is limited, details acquired from health data have varied uses since it contains the physical address of the data subject, his social security number, particulars of the employer, and insurance among others. Such details can be used to create a new credit card or take a bank loan. Hence over the dark web, electronic health data is sold for at least 20 American dollars while the credit card information fetches only 2 dollars.[16]

The breach of health data could leave a permanent impact on the data subject for instance while financial information such as credit card numbers could be changed, the information accessed from the electronic health records such as employer and residential address cannot be replaced. Thus signifying the gravity of electronic health data breach.[17]

While for a long time, it has been assumed that a breach of health data is solely a concern for the Global North, the Global South has witnessed a dramatic increase in data breaches with grave consequences for instance recently, a ransomware group attacked one of the premier medical institutions in India – All India Institute of Medical Sciences and made away with at least data of 30 million patients and encrypted the records rendering them inaccessible for 14 days.[18]

III. Human Rights Implications

The breach of personal data can be in many forms. It can range from simple breaches such as inadvertently giving access or exposing data to unauthorised persons apart from the one officially designated to handle it. In the context of health or learning institutions where persons are drawn from all walks of life when private information falls into the wrong hands, there are dire consequences. The data accessed could contain personal information such as the medical conditions of some persons for instance their HIV/AIDS status, allergies, and mental health issues among others. Such unlawful disclosure of personal information could

[12]Mary Wambui, "Hospitals Under Major Threat of Hackers", *Daily Nation*, 2020. Obtained on 23/06/2022 from; <https://nation.africa/kenya/news/hospitals-under-major-threat-of-hackers--3022062?view=htmlamp>

[13] Cyber Security and Infrastructure Security Agency, "Ransomware Activity Targeting the Healthcare and Public Health Sector", *Government of the United States of America*, Alert (AA20-302A). Obtained on 4/23/2022 from <https://www.cisa.gov/uscert/ncas/alerts/aa20-302a>

[14]Office of Information Security, "Hive Ransomware", *Government of United States of America*, White Report:202204181300. Obtained on 5/23/2022 from <https://www.hhs.gov/sites/default/files/hive-ransomware-analyst-note-tlpwhite.pdf>

[15]Hussain, *note 2*,p.134.

[16] Stephanie Domas, "Protecting Medical Devices from Cyberharm", TEDxColumbus (2016). Obtained from <https://www.youtube.com/watch?v=EyqwUFJKZo0&ab_channel=TEDxTalks> on 2308/2022.

[17]*Ibid*.

[18]Rai Shivangi, Shefali Malhotra, and Vivek Divan, "Digital Technology, Health & The Law Implications for Universal Health Coverage", *C-HELP Centre for Health Equity, Law and Policy,RTH-UHC Working Paper 4*, (2023), pp. 1-76 at p.13.

subject them to stigma, bias and discrimination to the extent that their ability to go on with their normal life is disrupted.[19]

Further, the handling of big health data by both the state and private sector has come under the microscope. While the private health sector has been accused of allowing unauthorised access to health data to monetise it, on the other hand, human rights stakeholders have pointed an accusing finger at the State for taking advantage of health emergencies such as COVID-19 to infringe the human right to privacy.[20]

Various States including the United Kingdom, Ecuador, Israel and China created digital mechanisms for tracing individuals who could have come into contact with persons who had shown symptoms of covid-19. While this move played a significant role in helping curb the spread of the pandemic, concerns were raised about the handling of sensitive data collected especially considering that some of these States lacked legislation to guide the collection and processing of such information and they also did not have an oversight body to audit the handling of the health data. Moreover, some of these governments invested in private ventures to further this responsibility thereby raising concerns as to the possibility of personal sensitive data being monetised without consent or falling into wrong hands. For instance, the data contained even the geo-location of persons dwelling within the territories of the States.[21]

In addition to the above, the collection of this sensitive data for contact tracing and relaying of prompt messages to the people's electronic devices without proper oversight predisposed the data for other State purposes which were not authorised by the data subject for instance the checking of their immigration status hence increasing the possibility of infringement of the rights of vulnerable groups such as refugees, asylum seekers and immigrants in times of crises. [22]

Unauthorised access to sensitive personal information such as electronic health data can cause unbearable effects on the data subject. It can expose the individual to blackmail thereby causing untold mental health effects and financial hardship. For instance, the unauthorised access to the data subject's medical history exposes sensitive details which could cause significant damage. Information such as mental health conditions, abortions or sexually transmitted diseases if leaked to the public or shared with colleagues at the workplace, classmates, family members or friends could lead to embarrassment, stigma, isolation, ostracisation, discrimination and potentially violence, from others who may hold discriminatory attitudes towards some of these conditions. It could be worse if the data subject hails from a conservative society but even in communities that tend to care little about other people's lifestyles- the laissez-faire attitude; the disclosure of such sensitive information increases chances of indirect bias and stigma.[23]

IV. A Human Rights Perspective for Enhancing Health Data Protection in the Global South

Various international and regional treaties on the right to health oblige States to ensure the proper handling of health data. The main international treaty which provides for the human right to health requires States to respect, protect and provide aspects of this right.[24] The obligation to protect requires State parties to prevent any harm such as a breach of health data that may arise in the course of the enjoyment of this fundamental right.[25] Additionally, the State is obliged to come up with mechanisms to prevent any form of discrimination, especially based on a person's race[26] or any form of discrimination against women.[27] Apart from the above international and regional treaties also oblige the States to protect their citizens against any form of discrimination especially women considering that they are the most frequent victims of these forms of

[19]Sun Nina, Kenechukwu Esom, Mandeep Dhaliwal and Joseph J. Amon, "Human Rights and Digital Health Technologies", *Health and Human Rights,* vol.22(2020), pp.21-32 at p.25.
[20]Shivangi, *note 19,* p.1
[21]Nina, *note 20,* p.23.
[22]*Ibid.*
[23]Shivangi, *note 19,* p.13.
[24] International Covenant on Economic, Social and Cultural Rights, art. 12, adopted Dec. 1966, G.A. Res. 2200 (XXI), U.N. GAOR, 21st Sess., Supp. No. 16, U.N. Doc. A/6316 (1966), 993 U.N.T.S. 3 (entered into force 3 Jan.1976).
[25] Toebes Brigit, "Towards an Improved Understanding of the International Human Right to Health", *Human Rights Quarterly* vol. 21 (1999), pp. 661-679 at p.677.
[26]International Convention on the Elimination of All Forms of Racial Discrimination, art. 5(e)(iv), adopted 21 Dec. 1965, 660 U.N.T.S. 195 (entered into force 4 Jan. 1969), reprinted in 5 I.L.M. 352 (1966).
[27] Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa, art 3, (adopted 11 July 2003, entered into force 25 November 2005) OAU Doc. CAB/LEG/66.6 (2003).

discrimination.[28] Above all, the international legal framework obliges State parties to ensure that "their citizens are not subjected to unlawful interference of their privacy nor should they be subjected to unlawful attacks that will damage their owner and reputation."[29]

It should be noted that various pacts obligating States to set up data protections have been enacted including the Convention on Cyber Security and Personal Data Protection, Asia-Pacific Economic Cooperation Privacy Framework, European Union's General Data Protection Regulation, Standards for Personal Data Protection for Ibero-American States, and Council of Europe's Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data. However, concerns have been raised that many jurisdictions have not effectively implemented their obligations in this regard. While jurisdictions such as the European Union have put in place robust mechanisms that compel data handlers to adhere to strict guidelines, this has not been replicated in the Global South as many States have not reviewed or updated their data laws and regulations to suit the current technological shifts. Additionally, for those that have put in place the desired legal mechanisms, their implementation has not been adequate hence exposing their citizens to personal data breaches consequently leading to infringement of their rights.[30]

The European Union General Data Protection Regulation has received glowing tributes globally for its authoritative nature as it prescribes stringent obligations to entities handling personal data to ensure the rights of the individual are not breached. Moreover, in line with these times when artificial intelligence is in vogue, the statute grants the individual the right to object to having his data subjected to automation practices for instance-profiling.[31]

Eminent jurists have opined that the setting up of legal mechanisms for data handling should embrace a human rights approach while upholding the following principles. The first of these is informed consent which is obtained devoid of any form of coercion. The document or person seeking consent should detail such request in plain and understandable language. Further, it should detail what kind of data is being collected and what would be its purpose. Additionally, entities handling the data should ensure that requisite safeguards are put in place to ensure the security of such data. The Supreme Court of India has shed light on handling personal data in the decision of *Justice K.S. Puttaswamy (Rtd) v. Union of India and Others* in which the apex bench held that privacy is a fundamental human right as it gives the individual the power to exercise control over himself and it provides necessary conditions for the enjoyment of other fundamental rights. The court underlined that individuals have the right to have their health data protected as part of the right to privacy.[32]

Therefore, the State is under obligation to enact statutes and implement mechanisms which provide safeguards for the prevention of unauthorised access or disclosure of health data.[33] It should be underlined in the formulation of these laws, regulations or guidelines the State should embrace a human rights approach in dispensing its obligations espoused therein.[34]

Although there is no express statute for the protection of the right to the protection of health data, the precedent-setting decision of the apex court in *Justice K.S. Puttaswamy (Rtd) v. Union of India* read with other statutes obliges the Indian government to provide this protection.[35] The other statutes include the Information Technology Act and Rules 2011 The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 issued under the eponymous Act, which corroborates the recognition of sensitive personal data to include "physical, physiological and mental health conditions, sexual orientation and medical records."[36] Additionally, the HIV/AIDS (Prevention and Control) Act, 2017 details requirements for Indian State agencies handling HIV-related personal data to put up stringent

[28]Convention on the Elimination of All Forms of Discrimination Against Women, art. 12, adopted 18 Dec. 1979, G.A. Res. 34/180, U.N. GAOR, 34th Sess., Supp. No. 46, U.N. Doc. A/34/46 (1980) (entered into force 3 Sept. 1981), reprinted in 19 I.L.M. 33 (1980).

[29] International Covenant on Civil and Political Rights, art.17, (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

[30]Nina, *note 20*, p.26.

[31] Regulation 2016/679 (General Data Protection Regulation), OJ L 119/1, art 22.

[32]*K. S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012.

[33]*Z v. Finland*: Application No. 22009/93 ECHR 10; European Court of Human Rights: Strasbourg, France, 1997.

[34] Florence A. Ogonjo, Rachel Achieng, and Margret Zalo, "An Overview of Data Protection in Kenyan Health Sector," *Strathmore University Centre for Intellectual Property and Information Technology Law* (2022), pp. 1-17 at p.11.

[35]*K. S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012.

[36] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, sec. 3.

mechanisms to ensure that the data is handled confidentially and protected from any form of breach or unauthorised disclosure.[37]

Besides the above, as held in *Shreya Singhal v Union of India*, in detailing the intended purpose of the data to be collected, the person proposing to collect the data must not only ensure that the purpose is lawful but also should ensure that the purpose is clearly stated because it being lawful is not clear enough. Similarly, when enacting data protection laws, the State should ensure that its provisions on the lawful purpose of collection of data are neither overbroad, vague nor arbitrary.[38] Above all, the Digital Personal Data Protection Act, of 2023, a proposed bill which is under parliamentary consideration has been touted as an extensive statute that will effectively regulate the processing of personal data of individuals by entities operating in India and abroad. It is hoped that upon receiving presidential assent, the government of India will fully implement it for the full protection of the health data of its citizens.[39]

In Sub-Saharan Africa, Kenya boasts one of the most robust health data protection statutes. Apart from other subsidiary legislations, the Data Protection Act sets a higher threshold for seeking consent than before. In seeking to collect data, a handler claiming to have sought consent has to establish that such permission has been obtained in an express, unequivocal, free, specific and informed manner by a clear affirmative action. Further, the statute requires persons who collect and handle personal information to anonymise the collected data by removing personal identifiers.[40]

The Act details the meaning of sensitive data as personal information detailing the health condition, race and sex of a person among others.[41] Further, it also underlines that when seeking data from a child, the consent of the minor's guardian should be sought.[42]

The provision for the establishment of the office of the Data Protection Commissioner, a quasi-judicial body that has the power to summon persons to appear before it and the power to mediate and conciliate parties and to impose fines[43] for breach of data raises the bar regarding the handling of personal information in the Global South. Further, the statute empowers the above body to make provisions for the regulation of the processing of personal data, the stipulation of the data producers' rights, and the specification of the obligations of the data controllers and processors.[44]

Additionally, the statute forbids any person from collecting, controlling or processing health data unless such persons are registered by the Data Commissioner.[45] Further, persons handling and processing the data are required to adhere to the right to privacy of the data subject.[46] In ensuring and promoting transparency in handling personal data, the Act requires persons whose data is to be collected to be notified and the purpose of such data made known.[47] Above all, the statute expressly details what type of data is to be considered health data and extra safeguards for handling this sensitive data including ensuring confidentiality.[48] While a lot remains to be seen, the Data Commissioner has already been appointed and has recently imposed fines on entities that make use of personal data without consent. This signifies the Commissioner's independence and resolve to hold to account persons infringing the right to protection of the sensitive data of citizens.[49]

V. Conclusion

[37] HIV/AIDS (Prevention and Control) Act 2017, sec. 11.
[38]Shreya Singhal v Union of India (2015) 5 SCC 1
[39] Generally, see, RaiShivangi, Shefali Malhotra, and Vivek Divan, "Digital Technology, Health & The Law Implications for Universal Health Coverage", *C-HELP Centre for Health Equity, Law and Policy,RTH-UHC Working Paper 4*, (2023), pp. 1-76.
[40] Data Protection Act (Kenya), 2019, sec 2.
[41] Data Protection Act (Kenya), 2019, secs 2,47.
[42]*Ibid.*, sec 33.
[43]*Ibid.*, sec 9.
[44]*Ibid.*, sec 6.
[45] Ibid., sec 18.
[46]*Ibid.*, sec 25.
[47]*Ibid.*, sec 29.
[48]*Ibid.*, sec 46.
[49]International Association of Privacy Professionals, Kenya's ODPC issues KES9.375M in data protection fines, 2022. Accessed on 13/10/2023 from <https://iapp.org/news/a/kenyas-odpc-issues-kes9-375m-in-data-protection-fines/#:~:text=375M%20in%20data%20protection%20fines,-schedule%20Sep%2026&text=Kenya's%20Office%20of%20the%20Data,nonconsensual%20uses%20of%20personal%20data.>

As the Global South gears its efforts towards the building of capacity for the enjoyment of the human right to health through Universal Health Coverage as one of the Sustainable Development Goals, attention should be taken to ensure the enactment of a rights-based legal framework for the protection of health data.

The breach of health data causes unauthorised access to sensitive personal information that could cause lifelong effects on the data subject. Therefore, health facilities and other facilities which could require medical records such as learning institutions should exercise extra caution by laying down proper mechanisms for protecting this data in the era of digitisation. Above all, it should be noted that incidences of health data breaches are increasing especially in the private sector, however, due to concerns that they will lose their reputation, few private entities report the breaches. Therefore, state agencies such as the Data Commissioner should take necessary steps to ensure prompt reporting of such breaches and while doing so, they should not overlook private entities. Finally, the State should afford the oversight body the requisite funds and human resources to ensure it has implemented its mandate in protecting the right to privacy. Above all, the judiciary should be aware of the exponential increase in data breaches and continue its activism for strict protection of private data.[50]

[50]Shivangi, *note 19*, p.13.