Austin Public Health

Open Access

Austin Publishing Group

Research Article

A Scoping Overview of Global Legislation on Data Privacy and Protection: What are the Implications for Data Use, Transfer, and Sharing in E-Health Research?

Wanjihia VW[1*]; Muriithi BK[2]; Kaneko S[3]

[1]Centre for Public Health Research, Kenya Medical Research Institute- Nairobi, Kenya

[2]Institute of Tropical Medicine, Nagasaki University-Kenya Medical Research Institute, Nairobi, Kenya

[3]Department of Eco-epidemiology, Institute of Tropical Medicine, Nagasaki University. Nagasaki, Japan

[*]**Corresponding author: Wanjihia VW**

Centre for Public Health Research, Kenya Medical Research Institute- Nairobi, Kenya.

Tel: +818046904156

Email: vwanjihia@kemri.go.ke

Received: September 11, 2024

Accepted: September 30, 2024

Published: October 07, 2024

Abstract

Integration of digital technologies into health-care is positively impacting health outcomes globally. Consequently, creating need for regulation to ensure proper usage and transfer of data in digital platforms, while promoting its protection and privacy of data subjects. This scoping review investigates state of data privacy and protection legislation globally and analyses its impact on eHealth research.

The review examines various legislations in terms of coverage, strengths, weaknesses and recommendations in the context of biomedical research. It employs a methodological framework based on PRISMA-ScR checklist.

Results indicate lack of harmonized data protection laws and robust data governance frameworks. There are limited safeguards to ensure security and ethical use of digital data in e-health research. There is also lack of clear legislation regarding the classification of encrypted data, and the need to simplify legal language to prevent non-compliance. Issues like, defining data subjects' rights to opt out of data processing, establishing a consential age for data use, and protecting children's data are inadequate in some legislations. There is also limited regulatory oversight, and insecure data transfer methods.

Recommendations emphasize the need to encourage global enhancement of privacy standards and to treat data protection as a fundamental human right. Enhanced data subject privacy will foster scientific collaboration. Enforceable data subject rights and responsibilities for data processors that extend beyond territorial boundaries are recommended. Balancing privacy and data subject rights with advancing digital health research is the way forward. Unified bilateral or multilateral agreements to enhance data protection laws will ensure cohesive data governance.

Keywords: Data privacy; Data transfer; E-health research; Data Protection Legislation

Introduction

Globally, there is a bid to transform health outcomes and take health research to new frontiers through electronic health (eHealth), by utilization of digital devices and technologies. E-health refers to Information Technology applications in health care, which also include m-health or the use of mobile technology for healthcare. It involves supporting public health practice using mobile devices, personal digital assistants and other wireless devices. Due to the shortage of healthcare workers in low-income settings, the adoption and use of eHealth and mHealth technologies are critical to enhancing equitable access to healthcare. Adopting digital technologies and innovations is providing health systems with capabilities for reaching vulnerable population groups [1,2]. E-Health has gained global acceptance because it is innovative, cost-effective and can deliver

Citation: Wanjihia VW, Muriithi BK, Kaneko S. A Scoping Overview of Global Legislation on Data Privacy and Protection: What are the Implications for Data Use, Transfer, and Sharing in E-Health Research?. Austin Public Health. 2024; 8(1): 1023.

health interventions and information to remote, hard-to-reach areas. Nevertheless, e-health may remain under-utilized due to economic and technological challenges. Other challenges also include low technology literacy amongst intended users, lack of interoperability of eHealth systems, market fragmentation, weak regulatory framework, and possibly lack of understanding on how to protect subjects' privacy and confidentiality [3-5].

That not-withstanding, it is important to explore the challenges and possible mitigations in data use and transfer, as well as data privacy and protection, especially since implementation of data protection laws has taken shape globally [6,7]. Mhealth and mobile technologies represent a promising tool to increase healthcare efficiency and enhance service utilization [8]. They support healthcare, where they provide two-way communication and access to many health resources [9,10]. Additionally, technologies like health applications (apps) can extend well beyond the boundaries of a physical contact environment, for patients or study participants, as well as healthcare providers and researchers [11-14].

The uptake and use of digital technology for healthcare or health research initiatives has led to the emergence of an innovative field of information technology in health. There are multiple stakeholders in this field of research, whose roles span from developing evidence-based mHealth interventions for a range of physical and mental health conditions as well as research applications [15-19]. While such applications substantially improve health care delivery and enhance research, there is a need for regulatory procedures to ensure proper usage and transfer of data held in these digital platforms, while ensuring the privacy and protection of the data subjects [20]. It is imperative for all stakeholders to understand that digital innovation also comes with digital risks that demand protective measures through Privacy Enhancing Technologies (PETs) such as the use of security software that supports encryption, firewalls, anonymization, spam filters, anti-virus and anti-spyware tools among others [21-23].

Digital health technology studies entail characteristics with which many researchers are unfamiliar and therefore, there should be close collaboration between various stakeholders at all phases of the digital project, which may involve various e-health strategies [24,25]. These may include but are not limited to, conducting familiarization with telecommunication infrastructure and commercial mobile service providers so that researchers will not find mHealth projects to be towering and complex or out of their scope [26]. It is therefore important to build the capacity of researchers collaborating between Low and Middle Income Countries (LMIC) and High Income Countries (HIC) as well so that they may align well with the emergence of Data Protection legislation in countries where digital research is conducted [27,28]. Explicably, data privacy can present ethical dilemmas in the digital realm. It remains key to understand how the data flows, is stored and is shared while at the same time safeguarding the right to confidential personal information. There is, therefore, need to assess eHealth policies and regulatory frameworks that can guide sustainable and balanced data sharing and data protection [29,30]. Additionally in eHealth, key to data privacy, is also data storage. Storage of data in the Cloud storage, where there is a shared virtual environment, or in an on-site server, managed by the data controller or outsourced to an IT provider, elicits a raft of novel problems. Researchers must guarantee the security of the participant information in the storage environment to avoid external attacks that may compromise the data [32].

Several countries have put in place laws to protect healthcare data. Among these is the United States of America, that developed the Health Insurance Portability and Accountability Act (HIPAA), which establishes national standards to protect an individual's identifiable health information, that was signed into effect in 1996. It emphasizes appropriate safeguards to protect health information and sets conditions on the use, disclosure and transmission to third parties that may be made of such information. Based on HIPAA, other countries have developed their own policies. The United Kingdom has the Data Protection Act of 2018 which controls how personal information is used by organisations, businesses or the government. The European Union, comprising of about 27 European Countries has General Data Protection Regulation (GDPR) which is a successor of the Data Protection Directive 95/46/EC which became defunct after the inception of the digital age. The GDPR which was enforced in 2018 aims to modernize data protection rules in the digital age, giving data subjects autonomy and a voice while dealing severely with entities that violate its guidelines. In Australia, security of healthcare data is ensured under Australian Privacy Principles under the Privacy Act of 1988. In Japan, the Protection of Personal Information (APPI) Act was promulgated in 2003 and was fully enforced in 2005. It established a basic framework for handling of personal information in the public and private sector. A separate act enacted to deal with health data aims to ensure that a data subject's information is processed anonymously and securely for research [33,34].

LMIC countries face substantial challenges regarding the privacy of personal data due to the requirement of sizeable funding and technology to implement structures. That notwithstanding, in 2014, the African Union (AU) Convention on Cyber Security and Personal Data Protection adopted a legal framework meant to address cybercrime and data protection in Africa. This is known as the Malabo Convention and it is an important tool for protection of personal data as well as preventing cybercrimes. It came into effect in June 2023, after fifteen African countries ratified it. (*Angola, Benin, Chad, Congo, Egypt, Gabon, Gambia, Guinea-Bissau, Lesotho, Mauritania, Namibia, Niger, Sao Tome and Principe, Senegal, and Zambia*) [35]

In Kenya, oversight of personal data is fragmented over a number of legislations; The Data Protection Act of 2019, under subsections 46 and 48, lays down the conditions for processing personal data related to health and possible transmission of that data to another country. Although the Act was enacted after the Kenya National E-Health policy of 2016-2030, they seem to work in tandem, since the e-health policy mandate is to protect and regulate the use of eHealth in the collection, retrieval, processing, storage, use and disclosure of personal health information albeit without giving specific mechanisms [36,37]. To enhance data governance, the Digital Health Act was enacted in 2023. This act recognizes data as a valuable asset in healthcare and health research and therefore defines transparent data use in three dimensions, of i) Value-why are the data collected? ii) Protection- How will data be stored, analysed and used? iii) Choice- How data governance works? [38,39].

This review focuses on utilization of digital technologies in health research and e-health as well as data privacy and protection in data use and transfer around the world. It examines the potential challenges and mitigations associated with balancing data usage and transfer while ensuring data privacy and protection. The review will explore issues such as adequacy of existing data protection measures, impact of data sharing on privacy, and effectiveness of safeguards in place. It aims to provide in-

sights into how institutions can navigate these complexities while ensuring sustainable collaboration and also to promote effective health research through digital technologies.

Methodology

The review was guided by the methodology outlined by [40,42]. A bibliographic search was carried out in the Pubmed database and online as well for publications on legislation addressing data protection and sharing, internationally. A hand search of websites and Google Scholar for articles and publications using key words was also done. The publications contained strengths and weaknesses in those legislations as far as data transfer and sharing, as well as data protection and privacy is concerned. The recommendations emanating from those publications were also explored.

The screening processes were guided by the research question, "**What are the various legislations for data privacy and security, challenges faced and the possible mitigations of the digital data use and transfer in e-health research?**" Only papers addressing data protection and transfer in eHealth research were included. Data extraction included publication title, year and type; country of legislation; challenges; benefits, Strengths, weaknesses, limitations, and recommendations. The results were reported using the PRISMA-ScR (Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews) checklist.

Results

The following six steps were observed: (1) identifying the research question; (2) identifying relevant studies; (3) study selection; (4) charting the data; (5) collating, summarizing, and reporting results; and (6) consultation. The PRISMA-ScR checklist was used to report the review results.

Initial search yielded 182 articles. Of these, 5 were duplicates leaving 177 articles that proceeded to screening. Screening process excluded 150 articles, leaving 27 articles that were considered for full-text review. Of these, 16 articles were included.

Table 1: Main results of the various legislations for data privacy and security, challenges faced and the possible mitigations of the digital data use and transfer in e-health research.

Author Ref. Year, Country	Type of Publication	Legislation	Purpose/coverage	Strengths	Weaknesses	Recommendation
(43,44) USA	Review Commentary	-HIPAA -Common Rule (CR)	-To protect the confidentiality and security of healthcare information (HIPAA) -To protect human subjects in federally funded research (CR)	-Making the informed consent process better for research participants (CR). -Protection of special populations in research (CR)	-Sometimes the informed consent process can be complex to decipher for patients if not well handled. (HIPAA) -Communication barriers and delays can arise due to fear of violations. (HIPAA) -Does not specify use of Private Health Information for Research Purposes (HIPAA)	-Inclusion of data governance clauses in informed consent documents. For instance, "Your data will be used for international/collaborative research and may be moved and stored in controlled-access databases meeting international security and safety standards in another country (ies)". -Holding data controllers accountable for violations of privacy and security.
(45) (46) Turkey	Research Article	Law on the Protection of Personal Data (LPPD)	-Gives data subjects control over their personal data. -Outlines obligations of data controllers. -Provides elaborate guidelines on data transfer to third parties.	-Notification of breach to oversight authority. - Provides for registration of data controllers.	-Does not provide territorial scope. -Does not set an age limit for consent. -Does not provide leeway for erasure of data.	-Revising of technical aspect of the health data management, terminologies, and regulations in Turkey especially for genetic/genomic testing. These should enable secondary use of data in compliance with FAIR (findable, accessible, interoperable, reusable).
(47) European Union (EU)	Review	General Data Protection Regulation (GDPR)	-Provides for rights of the data subject, duties of data controllers or processors and transfer of personal data to third countries (non-EEA countries). - Imposes penalties for breach of rights, security and privacy.	-Stipulates that a research participant/data subject can explicitly consent to a specific transfer of data after having been informed of the possible risks. -Stipulates that consent can be withdrawn any time, and blanket consent is not valid. -Stipulates that consent to data transfer is different from consent to research participation, as it may involve additional risk for the research participant, where there is the lack of appropriate safeguards.	-Has very high compliance costs. The implementation of structures is quite costly. -The penalties of non-compliance or breach are very high.	-Since not all countries possess a high standard of data protection, the European Union can encourage other countries to raise their privacy standards to a sustainable level. -The right to data protection should be treated as a fundamental right. -Granting research participants enforceable data subject rights and data processors, responsibilities that apply beyond territories. -Bilateral or multilateral negotiations and agreements for data protection standards when data are processed for biomedical research purposes.

(48) Switzerland	Research Article	1. The Federal Act on Data Protection (FADP) 2. The Human Research Act (HRA) and the Human Research Ordinance (HRO)	-Protecting fundamental rights and personal data processing of natural persons in Switzerland by private persons or federal bodies, in the private or public sector. -Regulates how personal data is collected, stored, used and transferred. 2. Governs research involving human beings.	-Researchers are allowed to disclose sensitive data for scientific reasons, as well as process it for further purposes. However, researchers must ensure that the data are rendered anonymous as soon as possible, so data subjects cannot be re-identified. -Informed consent is specific and does not give a blanket permission. -Data subjects have to be informed about anonymization and pseudomisation of data.	-Designation of a Data Protection Officer is not mandatory. -May not require explicit informed consent before processing data.	-Since most jurisdictions do not provide a clear definition about whether encrypted data represent a special category of data or whether it falls into the categories catered for, this should be clarified.
Canada		Personal Information Protection and Electronic Documents Act	-Sets the ground rules for how organizations collect, use, and disclose personal information.	-It allows data subjects to seek modifications or even erasure of their data. -It is not territorial in scope and applies even outside Canada.	-It has complex provisions and the cost of compliance may be prohibitive.	-Legislation should always be made easy to understand to avoid complexities which can be confusing and difficult to interpret. This will help to avoid compliance problems.
Australia (49)		(PIPEDA) Privacy Act	-Protects individuals in relation to their personal information.	-The Act covers external territories and also territories within Australia or Australia Privacy Principles (APP) entities. -Categorizes credit, tax and employee information as personal information. -Emphasises that de-identification does not remove the risk of re-identification.	-The Act does not consider IP Addresses as Personal Information. -Does not provide for keeping records of processing activities. -Does not define the need to appoint a Data Processing Officer. -Does not define privacy or terms of data protection.	-Should clearly define data subjects and give them greater autonomy to opt out of having their data processed. -Should also seek to establish consential age and provide more protection for the data of children.
(50) China	Brochure	Personal Information Privacy law (PIPL)	This law is targeted at personal information protection and preventing personal data leakage.	-Data subjects given more rights own data. Free to request to edit, remove, restrict the use of their data, or withdraw consent given previously. -Stipulates conducting of regular audits of processing activities and personal information protection impact assessments.	-Major social media cites in the world, are blocked in China.	While the PIPL contains many similarities to the GDPR, it is stricter on several fronts. Entities wishing to obtain or exchange data with China need specialised legal counsel.
(35) (51) Ratified by: Angola, Benin, Chad, Congo, Egypt, Gabon, Gambia, Guinea-Bissau, Lesotho, Mauritania, Namibia, Niger, Sao Tome and Principe, Senegal, and Zambia	Report/Convention	African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)	-The Malabo Convention recognizes the right to privacy. -Provides a framework for protecting personal data. -Signatories must establish data protection legislations and ensure that personal data is collected, processed, and stored securely.	-Emphasizes the importance of international or regional cooperation in curbing cybercrime and protecting personal data.	-The convention hinders data controllers from transferring personal data to a non-member state of the AU and they can only transfer personal data to a non-member state if the country has an adequate level of protection. - The convention is silent on health-related data.	- Ratification of an international/regional agreement leading to a unified legislation similar to the GDPR of EU, to provide for protection of personal data because even if the convention has 15 signatories so far, the particular legislations in the individual countries remain weak and not binding enough.

(52) (36) Kenya	Report	Data Protection Act, 2019	-To make provision for the regulation of the processing of personal data. -To provide for the rights of data subjects and obligations of data controllers and processors.	-Provides for registration of data controllers and data processors. -Recommends a data protection impact assessment. -Recommends data localization or storage of data in servers located within Kenya.	-Does not provide criteria for carrying out audits on the systems of data controllers and data processors.	-The Data Commissioner should develop clear guidelines for data controllers and data processors on the threshold required to undertake a data protection impact assessment. -Clarity must be made, in terms of the relationship or harmony of the Data Protection Act with other laws pertaining to data transfer in Kenya.
(53) Nigeria	Newsletter	Nigeria Data Protection Act (NDPA) 2023	-To regulate the processing of personal information and related issues.	-Has a retention principle where data processors establish clear data retention and deletion policies to ensure that they delete or anonymize data once it is no longer needed. -Provides that where a data subject is a child or lacks legal capacity, the data controller must obtain consent from a parent or legal guardian. -Data subjects have a right to revoke consent. -Precludes data controller or data processor from collecting and/ or processing data obtained through Automated Decision Making.	- Does not specify a timeframe for conducting a Data Protection Impact Assessment prior to processing the data of data subjects.	-Data Processors must assess their compliance status and strategies on evolving data protection policies. It becomes an even more complicated in the digital age due to machine learning, artificial intelligence, among others.
(54) South Africa	Act	Protection of Personal Information Act (POPIA)	-Defines personal data and prescribes duties for controllers and processors.	-Defines transparency to data subjects by data processors about data practices, lawful basis for processing, and implementation of appropriate safeguards to secure data and prevent data breaches.	-There is no fixed time frame for responding to data subject request.	-Establishment of a register for processing personal data.
(34) (55) Japan	Book Note	Act on the Protection of Personal Information (APPI) 2003	-This is the primary legislation that applies to the collection and processing of personal data.	-In case of a breach, there is a clear policy on informing the relevant authority as well as affected data subjects. - Has use of individual numbers known as “My number” that is supposed to streamline service delivery for everyone.	-Does not have a requirement for Data Protection Impact Assessment. -Does not provide the data subject with right of data portability or right to object to marketing and profiling. -Does not impose any obligations on data processors.	- A separate act exists to cover healthcare, research and medical strategy. A harmonization with the primary legislation is not clear.
Russia		Federal Law on Personal Data (No. 152-FZ), adopted in 2006.	It is the primary legislation governing the collection, processing, storage, and transfer of personal data in Russia.	-Specifies Personal data and also special categories under personal data. -Does not have a territorial limitation. -Has specifically defined categories of personal data.	-Provides for conditions where consent can be waived.	-Need to define the legal and ethical implications of using facial recognition and streamlining the requirement for certain types of personal data to be stored on servers located within Russia, which is facing challenges from businesses and international organizations. -There should also be addressing of concerns that the data protection law may conflict with other laws and regulations, such as those related to national security and law enforcement.

Discussion and Conclusion

The results indicate that data privacy and protection is getting prioritized all over the world and many countries have begun to craft relevant laws and regulations on handling personal information and data. The legislations set out the conditions that must be met in the processing of personal data, the rights of data subjects, the responsibilities of the various stakeholders involved in the processing of personal data, and the security requirements that must be met, among others. From these legislations, the safeguards that have been highlighted for data transfer are;

1. The country where the data is being transferred should have commensurate laws as the country of the origin of data or there should be adequate data protection laws in the recipient country.

2. There should be a contractual agreement between data regulatory bodies in the two countries exchanging data, using a harmonized template.

3. There should be consent from the data subject and this consent should meet the following criteria;

- **Voluntary and specific:** Consent should be given freely. It should not be obtained through any coercion or undue influence. The data subject must specifically understand **which** data is being collected and processed, for **what** objective, and by **whom**.

- **Informed:** The data processor or data controller must provide to the data subject, clear, concise and complete information about the data processing, including:

  - The **scope** of personal data or information that they are collecting.

  - The **objective** of processing the data.

  - The intended **recipients** of the data.

  - The data subject's **rights** regarding correction, access, rectification, and erasure of their data. Right to object to processing or transfer of their data and even the right to complain in case of perceived misuse of their data.

- **Explicit and documented:** Consent must be obtained in a clear way, in writing or electronic confirmation. Documenting the consent helps secure proof and evidence in case of future disputes.

- **Revocable:** Data subjects should have the right to withdraw their consent at any time without reprisals, and they should be provided with a simple and easily accessible method for doing so.

4. Permission from an established regulatory authority to carry out data transfer.

5. Encryption, anonymization, pseudonymization or removal of personal identifiable information before data transfer.

6. Data controllers and data processors should appoint Data Protection Officers in their various jurisdictions in order to provide stakeholders with guidance on data safety.

7. The Data commissioner to routinely carry out audits on the systems of data controllers and data processors.

In the context of international collaborative research, various regulations demonstrate that data may be moved and stored in controlled-access databases that meet international security and safety standards, even in other countries. In case of breach and to enhance accountability, during transfer, data controllers should be held accountable for violations of privacy and security.

In order to set global standards, countries with advanced data protection legislation, like the GDPR, of The European Union, can encourage other countries to elevate their data protection standards to sustainable levels through regional collaboration. Working towards unified legislations will be a key strategy for many countries, especially those from LMIC backgrounds for attaining international or regional agreement leading to unified legislation similar to the GDPR. Countries in Africa can negotiate around crafting a common data protection legislation that will protect the freedom and integrity of their people, based on the Malabo Convention.

The right to data protection should be a fundamental right everywhere in the world because data is a modern day gold mine which should be harnessed for the well-being of all people. Different jurisdictions should support enforceable rights of their data subjects, including research participants, and data processors should have responsibilities that apply beyond territories. Negotiations and agreements establishing bilateral or multilateral agreements for data protection standards in biomedical research should be emerging conversations in a technological new world. Simplified legislation that is straightforward to avoid complexities which may complicate compliance should also be encouraged.

Data Subject Autonomy has come out quite strongly in most legislations reviewed here and there has been an attempt to define data subjects clearly and give them greater autonomy to opt-out of data processing especially when automated decision-making is concerned. Protection for Children's Data has also come out strongly in a few legislations where they define the need to establish a consent age and provide additional protections for children's data. Specialized Legal Counsel have also been proposed where the penalties of non-compliance are quite heavy and punitive.

The need for Impact Assessments cannot be gainsaid as a safeguard for data transfer and some legislations have demonstrated the need to have Data Commissioners providing clear guidelines for data controllers and processors on data protection impact assessments.

In some countries, fragmented data protection laws have made compliance challenging. Harmonizing these laws could benefit the future of data protection and data transfer. Particularly, clarifying the relationship between separate acts covering healthcare, research, and medical strategy with primary legislation is essential to achieve this harmonization.

Under the provisions of the reviewed legislations, Institutional Review Boards (IRBs) which are primarily charged with approval of scientific research studies, especially among human subjects, should put up structures to enhance legal and ethical safeguards in digital data privacy and protection in the use of the data, it's sharing and transfer. It behoves IRBs to require that data handlers, data controllers and data processors in the realm of research, have consenting processes for data subjects that ensure proper safeguards for not only data use but also for data sharing and transfer, cross-boarders. Nevertheless,

privacy protection should not compromise research productivity, progress or scientific collaboration. Legal and ethical tools can facilitate digital scientific research while protecting the individual research participant or data subject. Research entities can practice full disclosure and enter into appropriate data use and data transfer agreements with data subjects, for the latter to give the required authorizations. Before consenting as research participants, data subjects should be well-informed and fully understand why the data is being collected, how and where it will be used, in which files and formats it will be stored and with what level of security and in case of any unauthorized security breaches, what steps will be taken. Informed consent documents should legitimately bear a data governance clause alluding to availability, usability, integrity, privacy and security of the data used.

Summary Recommendations

- **Global Enhancement of Privacy Standards**: Treat data protection as a fundamental human right and encourage globally synchronized privacy standards.

- **Enforceable Data Subject Rights**: Establish enforceable rights for data subjects and responsibilities for data processors that extend beyond territorial boundaries.

- **Unified Agreements**: Promote bilateral or multilateral agreements to enhance data protection laws and ensure cohesive data governance.

- **Simplified Legislation**: Make legislation easy to understand to avoid non-compliance and complexities.

Author Statements

Acknowledgement

This work was supported by the Japan Society for Promotion of Science (JSPS) FY 2024 Invitational Fellowships for Research in Japan (Long-term: L24521 to Satoshi Kaneko at Nagasaki University).

References

1. Ministry of Health. Kenya National e-health policy 2016-2030. Nairobi; 2016.

2. KENYA NATIONAL eHEALTH POLICY. 2016-2030.

3. Meyer AJ, Armstrong-Hough M, Babirye D, Mark D, Turimumahoro P, Ayakaka I, et al. Implementing mhealth interventions in a resource-constrained setting: Case study from Uganda. JMIR Mhealth Uhealth. 2020; 8: e19552.

4. Labrique AB, Wadhwani C, Williams KA, Lamptey P, Hesp C, Luk R, et al. Best practices in scaling digital health in low and middle income countries. Vol. 14, Globalization and Health. BioMed Central Ltd. 2018; 14: 103.

5. Aranda-Jan CB, Mohutsiwa-Dibe N, Loukanova S. Systematic review on what works, what does not work and why of implementation of mobile health (mHealth) projects in Africa. BMC Public Health. 2014; 14: 188.

6. Obasola OI, Mabawonku I, Lagunju I. A Review of e-Health Interventions for Maternal and Child Health in Sub-Sahara Africa. Vol. 19, Maternal and Child Health Journal. Springer New York LLC. 2015; 19: 1813–24.

7. Garg T, Kagalwalla N. Challenges of Implementing Privacy Policies Across the Globe. In: Data Protection and Privacy in Healthcare: Research and Innovations. 2021.

8. Pesando LM, Qiyomiddin K. Mobile phones and infant health at birth. Ortega JA, editor. PLoS One. 2023; 18: e0288089.

9. Lee SH, Nurmatov UB, Nwaru BI, Mukherjee M, Grant L, Pagliari C. Effectiveness of mHealth interventions for maternal, newborn and child health in low- and middle-income countries: Systematic review and meta-analysis. J Glob Health. 2016; 6: 010401.

10. Joshi V, Joshi NK, Bhardwaj P, Singh K, Ojha D, Jain YK. The Health Impact of mHealth Interventions in India: Systematic Review and Meta-Analysis. Online J Public Health Inform. 2023; 15: e50927.

11. Linde DS, Korsholm M, Katanga J, Rasch V, Lundh A, Andersen MS. One-way SMS and healthcare outcomes in Africa: Systematic review of randomised trials with meta-analysis. PLoS One. 2019; 14: e0217485.

12. Bossman E, Johansen MA, Zanaboni P. mHealth interventions to reduce maternal and child mortality in Sub-Saharan Africa and Southern Asia: A systematic literature review. Front Glob Women's Heal. 2022; 3.

13. Feroz A, Jabeen R, Saleem S. Using mobile phones to improve community health workers performance in low-and-middle-income countries. BMC Public Health. BioMed Central Ltd. 2020; 20: 49.

14. Chawla D, Thukral A, Kumar P, Deorari A. Harnessing mobile technology to deliver evidence-based maternal-infant care. Semin Fetal Neonatal Med. 2021; 26: 101206.

15. Martinez-Perez B, de la Torre-Diez I, Lopez-Coronado M. Mobile health applications for the most prevalent conditions by the World Health Organization: review and analysis. J Med Internet Res. 2013; 14: e120.

16. Kumar B, Singh SP, Mohan A. Emerging mobile communication technologies for health. In: 2010 International Conference on Computer and Communication Technology (ICCCT). Allahabad, India: Institute of Electrical and Electronics Engineers. 2010: 828–32.

17. Gupta R, Mitra M. Wireless Electrocardiogram Transmission in ISM Band: An Approach Towards Telecardiology. J Med Syst. 2014; 38: 90.

18. Bert F, Giacometti M, Gualano MR, Siliquini R. Smartphones and health promotion: A review of the evidence. J Med Syst. 2014; 38: 9995.

19. WHO Global Observatory for eHealth. MHealth : new horizons for health through mobile technologies. World Health Organization. 2011: 102.

20. Arora S, Yttri J, Nilsen W. Privacy and Security in Mobile Health (mHealth) Research. Alcohol Res. 2014; 36: 143–52.

21. Hussein R, Griffin AC, Pichon A, Oldenburg J. A guiding framework for creating a comprehensive strategy for mHealth data sharing, privacy, and governance in low- and middle-income countries (LMICs). Journal of the American Medical Informatics Association. Oxford University Press. 2023; 30: 787–94.

22. Li X, Wen Q, Li W, Zhang H, Jin Z. Secure Privacy-Preserving Biometric Authentication Scheme for Telecare Medicine Information Systems. J Med Syst. 2014; 38: 139.

23. Kumari K, Sharma A, Chakraborty C, Ananyaa M. Preserving Health Care Data Security and Privacy Using Carmichael's Theorem-Based Homomorphic Encryption and Modified Enhanced Homomorphic Encryption Schemes in Edge Computing Systems. J Big Data. 2022; 10: 1-17.

24. Filkins B, Kim JY, Roberts B, Armstrong W, Miller MA, Hultner ML, et al. Privacy and security in the era of digital health: what should translational researchers know and do about it? Am J Transl Res. 2016; 8: 1560–80.

25. Quach S, Thaichon P, Martin KD, Weaven S, Palmatier RW. Digi-

tal technologies: tensions in privacy and data. J Acad Mark Sci. 2022; 50: 1299–323.

26. Ben-Zeev D, Schueller SM, Begale M, Duffecy J, Kane JM, Mohr DC. Strategies for mHealth Research: Lessons from 3 Mobile Intervention Studies. Administration and Policy in Mental Health and Mental Health Services Research. 2015; 42: 157–67.

27. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. J Big Data. 2018; 5: 1.

28. Evertsz N, Bull S, Pratt B. What constitutes equitable data sharing in global health research? A scoping review of the literature on low-income and middle-income country stakeholders' perspectives. BMJ Glob Health. 2023; 8.

29. Bull S, Roberts N, Parker M. Views of Ethical Best Practices in Sharing Individual-Level Data from Medical and Public Health Research: A Systematic Scoping Review. Journal of Empirical Research on Human Research Ethics. 2015; 10: 225–38.

30. Waithira N, Mutinda B, Cheah PY. Data management and sharing policy: The first step towards promoting data sharing. BMC Medicine. BioMed Central Ltd. 2019; 17: 80.

31. Hussain M, Al-Haiqi A, Zaidan AA, Zaidan BB, Kiah M, Iqbal S, et al. A security framework for mHealth apps on Android platform. Comput Secur. 2018; 75: 191–217.

32. Rodrigues J, de la Torre I, Fernandez G, Lopez-Coronado M. Analysis of the security and privacy requirements of cloud-based electronic health records systems. J Med Internet Res. 2013; 15: e186.

33. Tzanou M. The GDPR and Big health data. In: Tzanou M, editor. Health Data Privacy under the GDPR: Big Data Challenges and regulatory Responses. 1st Edition. Taylor & Francis. 2021: 3–22.

34. Asai T. Japan Data Protection Law: A practical Guide comparison with the GDPR. 2nd Edition. 2022.

35. African Union. African Union convention on cyber security and personal data protection. Addis Ababa; 2000.

36. National Council for Law Reporting Republic of Kenya Kenya Gazette Supplement.

37. Kenya National Ehealth Policy 2016-2030.

38. The Digital Health Bill, 2023 Arrangement of Clauses. 2023.

39. Jamieson T, Salinas G. Protecting Human Subjects in the Digital Age: Issues and Best Practices of Data Protection. Surv Pract. 2018; 11: 1–10.

40. Arksey H, O'Malley L. Scoping studies: towards a methodological framework. Int J Soc Res Methodol. 2005: 19-32.

41. Levac D, Colquhoun H, O'Brien KK. Scoping studies: Advancing the methodology. Implementation Science. 2010; 5: 69.

42. Munn Z, Peters MDJ, Stern C, Tufanaru C, McArthur A, Aromataris E. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Med Res Methodol. 2018; 18: 143.

43. Majumder MA. United States: law and policy concerning transfer of genomic data to third countries. Vol. 137, Human Genetics. Springer Verlag. 2018; 137: 647–55.

44. DeRenzo EG, Moss J, Singer EA. Implications of the Revised Common Rule for Human Participant Research. Chest. 2019; 155: 272–8.

45. Şık AS, Aydınoğlu AU, Aydın Son Y. Assessing the readiness of Turkish health information systems for integrating genetic/genomic patient data: System architecture and available terminologies, legislative, and protection of personal data. Health Policy (New York). 2021; 125: 203–12.

46. Kinikoglu B. Implementing a new data protection law: lessons from the Turkish experience. Int Data Priv Law. 2023; 13: 25–46.

47. Bentzen HB. Exchange of Human Data Across International Boundaries. 2022.

48. Scheibner J, Ienca M, Kechagia S, Troncoso-Pastoriza JR, Raisaro JL, Hubaux JP, et al. Data protection and ethics requirements for multisite research with health data: A comparative examination of legislative governance frameworks and the role of data protection technologies. J Law Biosci. 2020; 7: lsaa010.

49. Government of Canada. Personal information protection and electronic documents act. Canada. 2019; 1–68.

50. Deloitte. China draft Personal Information Protection Law (PIPL) General introduction and impact analysis. Shanghai. 2021.

51. Malabo Convention.

52. Analysis of Kenya Data Protection Act, 2019_Jan2020.

53. The Nigeria Data Protection Act, 2023.

54. Government Gazette REPUBLIC OF SOUTH AFRICA P ARLIAMENT of the Republic of South Africa therefore enacts, as follows: CONTENTS OF ACT. 2013.

55. Sakai A. A GUIDE TO DATA PROTECTION IN JAPAN 202009. 2020.