NIU Journal of Legal Studies Copyright©2026
Nexus International University ISSN: *3007-1860;* 12(2): 5-22

Balancing User Trust and Mental Health Outcomes: A Comparative Analysis of Data Privacy Practices in Nigerian Mental Health Apps and the EU's GDPR

OGHOMWEN RITA OHIRO, UBOSE OSONAME OLORUNFEMI
University of Benin, Benin City, Nigeria

Abstract. The increasing use of mental health apps in Nigeria has the potential to improve access to mental health services, but this also raises concerns about data security and protection. Concerns about data privacy, lack of adequate regulation and cultural stigma in the long run chip away at users' trust of those apps and raise doubts about their efficacy in providing support to those in need. This study examined the relationship between data privacy policies and the use of mental health apps in Nigeria, focusing on how data protection laws influence users' attitudes. The paper examines the existing legal framework, including the Nigeria Data Protection Act 2023 and compares it with other regulatory regimes such as the General Data Protection Regulation in Europe and the Protection of Personal Information Act in South Africa. In this paper empirical research on current data collection practices and privacy issues in mental health applications are reviewed. The findings suggest that despite the considerable advances in regulations in Nigeria, there are shortcomings in law enforcement, regulations based on the industry and guidance on handling of sensitive information offered by users of mental health apps. These limitations result in a lower user trust and reduced app efficacy. The paper underscores the necessity of clarifying regulatory guidelines, adopting privacy-by-design principles, and addressing sociocultural factors to enhance the effectiveness of mental health applications in Nigeria.

Keywords: Data privacy, mental health apps, user trust, personal data, privacy by design

1. Introduction

Rapid proliferation of digital mental health apps across the world has provided immense opportunities in terms of increasing the reach and accessibility of mental healthcare, but at the same time, it has sparked concerns related to privacy and data protection.[1] The nature of mental health data is very delicate since it comprises of information relating to personal thoughts, histories of mental health conditions, emotions, etc. Therefore, misusing this data or making it accessible could be detrimental.[2] Some of the most stringent data protection systems existing today in relation to protecting information pertaining to mental well-being can be identified as those prevailing in Europe based on the General Data Protection Regulation[3] system.[4] Under the GDPR, mental health information is termed "special category data," thereby mandating informed consent on the part of patients along with strict data protection measures.[5] Likewise, similar provisions have been made in South Africa with the passing of the Protection of Personal

1 Johanna Löchner and others, 'Digital Interventions in Mental Health: An Overview and Future Perspectives, Internet Interventions' (2025) 40, https://doi.org/10.1016/j.invent.2025.100824.

2 Alenezi Turner, 'Privacy And Ethics In Mental Health Data Management' (2024) 15(6) *Journal of Health & Medical* Informatics, 564

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. (hereafter referred to as GDPR).

4 Antonio Pesqueira and others 'EU Privacy Law and B2B Digital Manufacturing Platforms in Mental Health' (2025) 4(1) *Innovation and Green Development* https://doi.org/10.1016/j.igd.2024.100196.

5 GDPR, 4(15)

Information Act (POPIA), which also covers health data.[6]

In Nigeria, the adoption of mental health apps is increasing, driven by unmet needs in mental health service delivery and the stigma associated with traditional care pathways.[7] It has been submitted that there is a treatment gap between mental health care delivery and those who need the treatment.[8] This is due to shortage of professionals ('in a country of over 200 million people, Nigeria has only 250 psychiatrists'),[9] fueling the need to fill the gap, especially considering the deficiency of traditional health care delivery.[10] This makes digital technology one means by which treatment can reach users.[11]

But worries over confidentiality, weak regulatory enforcement and cultural dispositions have stalled user trust and uptake. The Nigeria Data Protection Act (NDPA) 2023[12] is a significant legislative development, providing for rights such as access, rectification, erasure and restrictions on automated decision making.[13] Also, there is the Nigerian Mental Health Act which was passed into law in 2023.[14] This Act makes provisions for the right to privacy, informed consent and others." However, scholars note that although such advances have been made, many Nigerian healthcare facilities lack the infrastructure and training to translate the law into practice on paper. More empirical work is needed to link "national policy aspirations to institutional realities," scholars argue.[15] They argue that without systematic implementation strategies, legal frameworks like the NDPA remain "largely formal rather than operational.[16] A recent study on healthcare facilities showed that 37% of healthcare workers were unaware of any incident response plan for data breaches, citing "insufficient resources" (53%) and "lack of awareness" (71%) as primary barriers to compliance.[17]. Bagudu highlights that "loopholes still persist" in the enforcement of the NDPA. [18]He notes that the constant breach of data in Nigeria raises questions about the law's actual ability to guarantee privacy in practice, particularly in the era of the Internet of Things (IoT) where health data is increasingly digitalised.[19]

These shortcomings raise questions about whether Nigeria's framework can adequately protect mental health data and foster trust in digital platforms. There is also the issue of trust which is central to the adoption of mental health technologies. Studies show that privacy concerns are a critical barrier to engagement, with users often caught in a "privacy paradox": desiring help but fearing exposure.[20] In contexts like Nigeria, where stigma remains deeply entrenched, privacy protections are not peripheral but foundational to whether digital mental health tools can function as meaningful access points for care.[21]

---

6 Protection of Personal Information Government Gazette Republic of South Africa Vol. 581 No. 4 2013 <https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf> accessed 9 December 2026

7 Chinyere Okoroafor, 'Mental Health Advocates Turn to Technology to reach African Youths' February 18, 2026 The Nation <https://thenationonlineng.net/mental-health-advocates-turn-to-technology-to-reach-african-youths/> accessed 8 May 2026

8 A. O. Onwudiwe, 'Digital Mental Health: Integrating Psychotherapeutic Innovations and Technology—A Nigerian Perspective' (2025) 35(6) *Journal of Psychology in Africa* 843-851.

9 Sakeenah Kareem, 'Beyond the Mental Health Act: How an AI app is Filling Nigeria's Therapy Gap' (2026) *Campus Reporter Africa* <https://campusreporter.africa/beyond-the-mental-health-act-how-an-ai-app-is-filling-nigerias-therapy-gap/> accessed 8 May 2026

10 Onwudiwe, (n8).

11 Ibid.

12 The Nigeria Data Protection Act 2023 Federal Republic of Nigeria Official Gazette No.119 Vol. 110 (1 July 2023). The Act was enacted on 12 June 2023. 'President Tinubu Signs Data Protection Bill In Nigeria Into Law' *Sahara Reporters* (14 June 2023) <https://saharareporters.com/2023/06/14/president-tinubu-signs-data-protection-bill-nigeria-law> accessed 28 June 2025

13 NDPA 2023, part VI

14 Nigerian Mental Health Act, 2021, s. 19 and 26

15 B Idoko, 'Enhancing Healthcare Data Privacy and Security: A comparative study of regulations and best practices in the US and Nigeria' (2024) 11(2) *Magna Scientia Advanced Research and Reviews*, 151–167.

16 Ibid.

17 Krystal Chinenye Ugwu-Anyanwu and others, 'Assessment of Compliance with Data Protection and Privacy Regulations in the Nigeria Healthcare Sector' (2025) 1(1) *SIAR-Global Journal of Computer Information and Library Science* 128.

18 Haruna Abubakar Bagudu, 'Legal and Institutional Challenges to the Enforcement of the Nigerian Data Protection Act' (2026) *UDUS Law Journal* 291-295.

19 Ibid.

20 N Gerber, P Gerber, and M Volkamer, 'Explaining the Privacy Paradox: A Systematic Review' (2018) 77 *Computers & Security* 226–261.

21 Kareem, (n 9).

Against this backdrop, this paper examines the relationship between data privacy practices and user trust in Nigerian mental health applications, situating the NDPA 2023 within a comparative analysis of GDPR and POPIA. By reviewing empirical literature and regulatory frameworks, the study highlights both the progress and limitations of Nigeria's approach, emphasizing the need for privacy-by-design principles, sector-specific standards, and culturally sensitive safeguards. Ultimately, the paper argues that strengthening data protection in Nigeria is essential not only for compliance but also for improving mental health outcomes by fostering trust, reducing stigma, and ensuring equitable access to digital care.

2. Conceptual Framework: Data Privacy, Trust, and Digital Mental Health Use

This study conceptualises the relationship between data privacy regulation, user trust, and digital mental health utilisation as a structured causal chain in which legal frameworks shape behavioural outcomes through institutional credibility and perceived risk.

(1) Data Privacy as Control Over Personal Information

Alan Westin defines privacy as: "the claim of individuals… to determine for themselves when, how, and to what extent information about them is communicated to others."[22] This conception is now embedded in legal doctrine. The protection of personal data as a fundamental right has been affirmed in cases such as: *S and Marper v United Kingdom* [23] and *Digital Rights Ireland Ltd v Minister for Communications*.[24] These decisions establish that processing of personal data must satisfy necessity and proportionality, particularly where sensitive data is involved.

In *S and Marper v United Kingdom,* the Court determined that indefinite storage of such data was a breach of the individual's right to privacy. The Court of Justice of the European Union has also rendered decisions regarding the invalidity of mass retention rules, such as *in Digital Rights Ireland Ltd v Minister for Communications*, on the basis of being disproportionate, as stated that processing must be justified and necessary in particular cases of sensitive information. In the context of mental health, the issue becomes magnified. Ohm argues that sensitive data such as health information, involves higher risks of both re-identification and harm.[25]

(2) User Trust as an Institutional and Psychological Construct

Trust goes beyond mere personal feeling and becomes an institutional expectation. According to Luhmann's theory, the sociological roots of trust lie in its ability to make complex situations simpler in uncertain times.[26] Likewise, Gambetta also explains that trust refers to the expectation that one will behave favourably or at least in a non-harmful manner in spite of any lack of surveillance on the other side.[27] Trust in digital spaces is thus dependent on legal protection and institutional enforceability of trust. The significance of institutional trust in digital governance has been established through the case of *Schrems v Data Protection Commissioner* [28]wherein it was highlighted that weak safeguards in data transfers lead to violation of the fundamental rights of individuals. This happens when there is a trust deficit in a digital system because of non-enforceable rights, unclear risks, and no sanctions on violations.

(3) Digital Mental Health Use as Behavioural Outcome

It has been proven through health behaviours research that people would not readily share their private data in contexts they consider unsafe.[29] As noted in the theory of contextual integrity developed by Nissenbaum, privacy is protected when flows of information align with context-related standards. It goes without saying that mental health data falls into the category of highly private data.[30] If confidentiality conditions are violated because of unclear policies, misuse of data or lack of appropriate protection measures, users can: leave the platform, not share their info, or opt out of digital mental health care services.

---

22 Alan F. Westin, *Privacy and Freedom* (Atheneum 1967)

23 (2008) 48 EHRR 50

24 (Joined Cases C-293/12 and C-594/12)

25 Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 *UCLA Law Review* 1701

26 Niklas Luhmann, *Trust and Power* (Polity Press 1979)

27 Diego Gambetta (ed), *Trust: Making and Breaking Cooperative Relations* (Blackwell 1988)

28 *Schrems v Data Protection Commissioner* (Case C-362/14)

29 Havva Nur Atalay and Şebnem Yücel, 'Decoding Privacy Concerns: the Role of Perceived Risk and Benefits in Personal Health Data Disclosure' (2024) 82(1): *Arch Public Health* 180.

30 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010).

3. Methodology

This paper adopts a doctrinal and comparative legal research methodology, supplemented by interdisciplinary insights from digital health, psychology, and information systems literature. First, a doctrinal analysis is employed to examine the legal frameworks governing data protection in Nigeria, with particular emphasis on the Nigeria Data Protection Act 2023 (NDPA) and the General Application and Implementation Directive (GAID) 2025. This involves a close reading of statutory provisions, regulatory guidelines, and relevant institutional mechanisms in order to assess the scope, structure, and limitations of the Nigerian data protection regime as it applies to mental health data and digital applications.

Secondly, this research adopts a comparative law perspective in analysing Nigeria's regime against two chosen jurisdictions: the European Union and South Africa. The GDPR framework of the European Union will be used as one of the comparative frameworks owing to its worldwide recognition and role as a benchmark for data protection laws especially in regard to sensitive data and higher risk operations. On the other hand, POPIA of South Africa will be chosen for comparison purposes because of the nature of the legal system in that country. Comparative law analysis will focus on three main aspects of data protection which include provisions about substantive legal protection (definitions, grounds for processing data and dealing with sensitive data), specific and sectoral regulation especially on matters related to digital health and mental health services, and the effective implementation of data protection rights.

The paper also reviews empirical and interdisciplinary literature on mental health applications, data privacy risks, and user trust. This includes the study of app data collection practices, privacy vulnerabilities, algorithmic bias, and the socio-cultural determinants of technology adoption. These sources are not employed to produce new empirical findings but to contextualize the legal analysis and to shed light on how regulatory frameworks interact with real user behaviour and perceptions. This study is therefore analytical rather than empirical, and its conclusions are interpretative. It does not aim to measure user trust directly but rather to explore how legal structures may affect the conditions under which trust is either promoted or damaged.

4. Data Privacy Landscape in Nigeria

In Nigeria, the 1999 Constitution of the Federal Republic of Nigeria (as amended),[31] the Nigeria Data Protection Act 2023, a few statutes, and subsidiary legislation essentially regulate data protection. Section 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended) provides that 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.'[32] The Nigeria Data Protection Act 2023 was enacted on 12 June 2023. Some of the objectives of this Act are to establish an effective regulatory framework for the protection of personal data, regulate the processing of information relating to data subjects, to safeguard their fundamental rights and freedoms as guaranteed under the 1999 Constitution of the Federal Republic of Nigeria (as amended), to establish an independent Commission to oversee data protection and privacy issues and to supervise data controllers and data processors among others.[33]

The NDPA 2023 is a comprehensive law, which offers some new rights to data subjects, such as the right not to be subject to automated decisions solely based on data processing.[34] The Nigeria Data Protection Act (NDPA) 2023 regulates organisations' processing of personal data.[35] It applies broadly to all processing methods, automated or not.[36] It covers organisations domiciled or operating in Nigeria, even if processing data from individuals outside the country.[37] There are exemptions for personal use, law enforcement, national security, and other reasons outlined in the Act (Section 3).

The NDPA 2023 is complemented by the General Application and Implementation Directive (GAID) 2025 issued by the Nigeria Data Protection Commission, which provides specific guidance on how to implement the Act. The GAID gives effect to key provisions of the NDPA by setting out requirements in relation to data processing including transparency obligations, lawful bases for processing,

31 See the Constitution of the Federal Republic of Nigeria 1999 (as amended), Act No.24, 5 May 1999, hereafter referred to as CFRN 1999

32 In addition, Section 39 of the CFRN 1999 (as amended) guarantees the right of every person to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference

33 Nigerian Data Protection Act 2023, s.1.

34 NDPA 2023, s.37(1)

35 Ibid, s.1

36 Ibid, s. 2(1)

37 Ibid, s.2(2)(a) - (c)

Data Privacy Impact Assessments and deployment of data processing software.[38] Therefore, the NDPA and the GAID must be read together to form the core of Nigeria's contemporary data protection framework.

The NDPA 2023 establishes core principles for data processing, requiring organizations to handle data lawfully, fairly, and transparently for specific purposes only.[39] Individuals have various rights under the Act, including the right to access, rectify, erase, and restrict the processing of their personal data.[40] They can also object to automated decision-making solely based on data processing and have the right to data portability, allowing them to move their data between organisations.[41]

For situations where data processing poses high risks to individuals, the Act mandates Data Protection Impact Assessments (DPIAs) before processing commence.[42] The Commission will provide further guidance on DPIA requirements.[43] In practice, this requirement has been further elaborated under the GAID 2025, which specifies circumstances such as healthcare services, sensitive personal data processing, and the deployment of digital applications as triggering mandatory DPIAs.[44]

The Act introduces "legitimate interest" as a justification for data processing, but leaves the term undefined, potentially causing confusion.[45] However, the GAID 2025 provides additional structure under Article 26 by requiring organisations to conduct Legitimate Interest Assessments and to apply principles such as necessity, proportionality, and duty of care, although the concept remains broadly framed in its application. The Act defines and sets conditions for processing sensitive personal data with the Commission empowered to add new categories in the future.[46]

The Nigeria Data Protection Act (NDPA) 2023 offers some provisions that could be effective for the protection of mental health, but it also has limitations. The provisions that could be effective are, for instance, the one that grants individuals the right to access, rectify, erase, and restrict the processing of their data.[47] This can empower people to control sensitive information related to mental health conditions. It is also instructive that the Act requires organisations to be transparent about collecting and using personal data.[48] A requirement further reinforced by Article 27 of the GAID, which mandates that such information must be clear, accessible, and understandable to data subjects. This can help individuals understand how their mental health data may be used. The Act mandates security measures to protect data from unauthorised access, loss, or destruction.[49] This helps safeguard sensitive mental health information from breaches.

The NDPA fails to provide adequate guidance on collecting and handling of mental health data especially in light of its application to digital media platforms such as mobile apps. While there is mention of Article 31 of the GAID which requires DPIA and embedding of privacy policy within the software, these terms are very general and lack specificity for mental health apps.

Additionally, it allows processing based on legitimate interest without specifying what this term means. The problem with this provision is that organizations can abuse it or misinterpret legitimate interest to handle mental health data when the proper approach would have been obtaining consent from Article 18 of GAID.

The Act grants individuals some basic rights regarding their personal information; it also has a number of enforcement provisions in the form of investigatory powers, compliance orders, [50] and administrative sanctions that can be applied by the Commission. These include fines for the harm caused by any data processing activity and can also include compensation for the individual affected or even an injunction against the processing of any personal data. [51] This is aimed at deterring non-compliance with the Act and giving individuals some remedy for any harm that they may have suffered. Fines can be imposed on individuals, organizations, bodies, or groups who process personal data in any way.[52] In addition, individuals can sue the data controller or processor for any damage that they have suffered because of the breach of their personal data. [53] This enables individuals to claim compensation for any damage done to their mental well-being. It is not clear from the

38 GAID, arts 27, 26, 28, 31.
39 Ibid, s.24(1)(a(and (b)
40 Ibid, s.34-36
41 Ibid, s.37(1) and 38
42 Ibid, s.28(1)
43 Ibid, s.28(3) – (4)
44 GAID, art 28(3)
45 Ibid, s.30(d)
46 Ibid, s.65 and 30 (2)
47 NDPA 2023, s.34-36
48 Ibid, s.24(1) (b)
49 Ibid, s.24(1)(f)
50 Ibid, s.46 and 47
51 Ibid, s.48
52 Ibid, s.48 and 49
53 Ibid, s.51

Act how priority will be given to mental health complaints by the Commission.[54]

However, the effectiveness of these mechanisms in practice remains dependent on the evolving institutional capacity and enforcement practices of the Nigeria Data Protection Commission. Notably, the Act requires individuals seeking damages to prove harm, a standard that may present significant challenges, particularly in relation to mental health matters. This can be difficult, especially for mental health issues.

In summary, the NDPA 2023 constitutes a positive development in the landscape of data protection in Nigeria. However, to ensure its effectiveness in safeguarding mental health data, further regulatory clarification and sector-specific guidance may be required. Potential areas for further development include:

- Developing sector-specific standards or guidance for mental health data processing, particularly in digital health applications.
- Clarifying the application and limits of legitimate interest in the context of sensitive personal data such as mental health information.
- Enhancing practical enforcement capacity and establishing clear regulatory priorities for high-risk data categories, including mental health data.

5. Relevant Data Protection Initiatives Related to the Digital Health Sector

5.1 The Nigerian Mental Health Act 2021

Although the NDPA 2023 has provided for a horizontal data protection regime with regard to personal data, the enactment of the National Mental Health Act 2021 ensures the provision of vital sectoral safeguards necessary considering the 'vulnerability' and 'high-risk' nature of mental health data as highlighted in this paper. The Act has been enacted as a replacement to the old Lunacy Act of 1958 that was introduced under colonial rule. This Act represents a shift from the country's rights-based approach, explicitly codifying privacy and confidentiality as fundamental clinical rights rather than just administrative obligations.

The Act provides dual-layer protection for information. Section 19 explicitly outlines the “Right to privacy and dignity” for persons with mental health conditions. Section 21 adds to this by creating a separate “Right to confidentiality” in respect of a patient’s medical condition and treatment history. For digital mental health applications, these provisions mean that any data breach is not just a regulatory failure under the NDPA but a direct violation of a patient’s statutory civil rights.

There is a provision for “Informed consent” under Section 26 of the Act. The Act requires that consent should be voluntary and made on the basis of an informed understanding of the nature of the treatment and its likely results. If this standard is applied in digital contexts, it adds weight to the claim that a broad “Terms of Service” or “Legitimate Interest” explanation used by applications is inadequate. As regards mental health data, the Act requires that the consent must be meaningful, given that the data is sensitive.

This Act creates the Department of Mental Health Services, whose sole responsibility is the gathering and dissemination of information about mental health, as well as conducting research.[55] Most importantly, Section 5(d) of the Act requires the Department to "guarantee the fundamental rights and safety of the patient." In other words, it ensures that users will be protected from any form of discrimination and stigma associated with their use of digital applications. In addition, the creation of a Mental Health Assessment Committee serves as a specialized system of dispute resolution.[56] The Committee has the authority to investigate claims about the abuse of individuals within the scope of the Act, which might offer an easier avenue of recourse than the general court system.[57]

5.2 The National Health Act 2014

The National Health Act 2014 provides that information concerning a user, including information relating to his health status, treatment or stay in a health establishment is confidential.[58] The National Health Act (NHA) 2014 has some effective provisions for mental health data, but there are also limitations to consider. There are effective provisions, for instance, the Act protects the confidentiality of user information, including mental health data.[59] This

54 Ibid, s.46
55 Nigerian Mental Health Act, s 2.
56 Ibid, s 9.
57 Ibid, s 11.
58 National Health Act, Federal Republic of Nigeria Official Gazette No.145 (27th October 2014) Vol. 101, (NHA 2014), s. 26(1)
59 Ibid, s.26(1)

safeguards sensitive information and protects patients from discrimination. Healthcare providers can access mental health data for treatment purposes with the patient's consent.[60] This ensures continuity of care. Patients can complain about how their mental health data is handled.[61] This empowers individuals to address potential breaches. The Act requires health facilities to implement security measures to protect health records, including mental health data.[62] This helps prevent unauthorized access. There are some provisions that may constitute limitations, for instance, consent for research or teaching that does not identify individuals does not require patient authorisation.[63] This could be misused for mental health data research without explicit consent.

Secondly, the Act focuses on health establishments, not data collection by other entities.[64] This leaves mental health data collected outside these settings (e.g., mental health apps) unprotected.
Overall, the NHA 2014 offers a basic framework for mental health data protection. However, it can be strengthened by:

- requiring explicit consent for using mental health data in research, even if anonymized,
- expanding the Act's scope to cover data collection by other entities that handle mental health information, and
- providing clearer definitions of key terms related to data protection.

By addressing these limitations, the NHA 2014 can become a more robust tool for safeguarding the privacy of mental health data in Nigeria.

5.3 Data Collection Practices in Mental Health Apps

Mobile health apps collect data through three main methods: built-in smartphone sensors (e.g., camera, microphone, GPS), external sensors (e.g., wearable devices) connected via Bluetooth and manual data entry by the user.[65] Most mental health apps rely on users to manually enter data rather than leveraging smartphone sensors or wearable devices.[66]

Data breaches in mental health applications are significantly more dangerous than in normal mobile applications.[67] This is due to the highly sensitive nature of the information associated with mental health. For example, the exposure of an individual's IMEI, UUID, or IP in the use of WhatsApp or Netflix may not be of much concern to people.[68] With respect to mental health applications, it is a severe violation of the user's privacy; users want their mental state to remain confidential.[69] In most cases, mere knowledge that an individual uses an application that deals with his/her mental well-being may already mean something significant to others.[70] This heightened risk underlines the need for stricter privacy protections and safeguards for mental health apps. Mental health apps pose unique data privacy risks due to the extra sensitivity of the information they handle.[71] Unlike general health apps for fitness or wellness, mental health apps deal with deeply personal details.[72] This creates a double threat:[73]

Security breaches can expose highly sensitive data: Information on mental health conditions is much more private than fitness data. A leak could have serious consequences.

Social stigma can be amplified by privacy violations: Mental health conditions still carry stigma. Even just knowing someone uses a mental health app could reveal that they are struggling, making them feel even more vulnerable.

Research that analysed top-ranked mental health apps (that require health and/or personal data as inputs to be functional and transmit users' data to a remote host) to understand how they handle data privacy has revealed significant data privacy problems including unnecessary app permissions, weak encryption methods, and leaks of personal data.[74] The apps lack mechanisms to prevent linking user data to

60 Ibid, s.28(1) (a)
61 Ibid, s.30
62 Ibid, s.29(1)
63 Ibid, 28(2)
64 NHA 2014, s.26
65 B. J. Phillip and others, 'Data Collection Mechanisms in Health and Wellness Apps: Review and Analysis' *Jmir Mhealth and Uhealth* (2022) 10(3) 2.
66 Ibid, 8; H. Wisniewski, 'Understanding the Quality, Effectiveness and Attributes of Top-Rated Smartphone Health Apps'(2019) 22(1) *Evidence Based Mental Health* 4-9.
67 L. H. Iwaya, 'On Mental Health Apps: An Empirical Investigation and Its Implications for App Development' *Empirical Software Engineering* (2023) 28.
68 Ibid.
69 Ibid.
70 Ibid.
71 Iwaya, (n 67).
72 Ibid.
73 Ibid.
74 Ibid, 1

individuals, increasing the risk of user profiling by developers or third parties.[75] The study found serious privacy issues in mental health apps, despite them being used by millions who likely expect strong privacy protections.[76] Some of these privacy issues include:

User tracking is very high risk: There is a possibility that many apps enable third-party entities to identify the person using them as well as track their actions.

Inadequate transparency: The privacy policies of many of these apps were too difficult to understand and did not warn about any risks such as targeted advertising based on mental problems or revealing one's illness.
Fewer apps had undergone any form of privacy impact assessments.

Difficult privacy policies: Nearly all privacy policies require advanced education to understand, making it hard for users to know how their data is handled.

Weak security: Static analysis revealed critical security risks in most apps, including weak encryption, and dynamic analysis showed some apps transmit sensitive data unencrypted, making it vulnerable to leaks.
Earning user trust is critical for digital health apps.[77] This starts with transparent and easy-to-understand explanations of how data is processed. Users should not be left wondering what is happening to their information. Users should have complete control over their health data. This means providing them with the ability to easily check what information is being collected about them at any given time. Empowering users is key. The app's user interface should be designed for transparency and allow users to effortlessly adjust their data privacy settings whenever they want.

6. Impact on User Behaviour and Mental Health Outcomes

6.1 Data Privacy Concerns and User Trust in Mental Health Apps

As a result of technological advancement, the question of data privacy and protection has gained more grounds in contemporary society. In respect to mental health sectors, technology has helped in the development of application software that cater for the mental needs of the larger society. This advancement conceptualizes the need of data privacy in relation to digital mental health, thus, its usage is not without skepticism. One of the major arguments against digital mental health apps is the privacy of the data of those who patronize these application tools. Prospective and willing users who patronize these apps are left with more worries as to the extent of security of their personal data, which in the long run is supposed to be built on trust between the credibility of these software applications (apps) and the extent of data protection. Trust becomes the driving requirement that facilitates the engagement of users. David Zhang and others argue that privacy concerns can serve as a critical barrier to adoption, directly undermining the very access to care that these platforms are designed to expand.[78]

Furthermore, these technological advanced mental health platforms in respect to privacy have been limited in their expansion, especially in Nigeria, as a result of its novelty and citizen's limited knowledge of data rights. In addition to these major concerns, the fear over disclosure of information has hindered the patronage of these platforms. However, the balance is debated between people to patronize these platforms than approach a mental health center where their data are also exposed to same risk as opening up to another person. This has been described as "privacy paradox". No doubts, Nigerians seems to be more woven in this paradoxical web. The fear of being found to have mental illness reduces interaction of these persons while they interact with tools before their personal information is not guaranteed safety. It has become a contest of being embarrassed and getting necessary help.[79]

---

75 Ibid.

76 Ibid.

77 T. J. Schwarz, 'GDPR Compliance for Digital Health Apps' < https://www.taylorwessing.com/en/insights-and-events/insights/2021/04/dsgvo-compliance-bei-digital-health-apps#:~:text=Because%20digital%20health%20apps%20often,of%20digital%20health%20apps%20(Art.> accessed 28 May 2024

78 D. Zhang, J. Lim, L. Zhou and A. Dahl, "Breaking the Data Value-Privacy Paradox in Mobile Mental Health Systems Through User-Centered Privacy Protection: A Web-Based Survey Study" (2021) 8(12) *JMIR Mental Health* e31633, <https://mental.jmir.org/2021/12/e31633> accessed 1 March 2026.

79 N. Gerber, P. Gerber and M. Volkamer, "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior" (2018) 77 *Computers & Security* 226–261.

In the same light, the effect on Nigerian men proves to be no better. A study which examined the barriers to mental health support among Nigerian men, discovered that men tend to avoid digital mental health apps where complex privacy policies, technical language and overly formal layout of the app are needed rather than explore the potential benefit of these apps in solving their issues. This gap can be traced to the trust deficit.[80] The danger this paradoxical web poses is that it devalues the very antidote that addresses mental health issues of potential users. Thus, leading to progressive depreciation of mental wellness of the potential users.

6.2 Cultural Factors, Stigma, and Perceptions of Data Privacy

Cultural predisposition and determines the extent to which individuals will accept the usage of digital mental health tools. Historically, issues of mental health have been associated more with spiritual attacks rather than a medical situation that requires critical care like any other disease or sickness.[81] This complicates the how the mental health issues are addressed in Nigerian society. Victims are stigmatized and left without care not to talk of the mind-set towards digital mental health apps and tools. It has become a double barrel gun for the users ,as they face the fear of public stigmatization and breach of data privacy while using tools.

Accordingly, research confirms that stigma surrounding mental illness in Nigeria is more of a culturally embedded social response than an individual attitude, which stems from shared beliefs about the causes and meanings of mental disorder.[82] In addition to this position, scholarship on technology-based mental health in Nigeria has observed that mental health tools have received more cultural bias as it negates the conventional mode of handling mental health cases.[83] With this in mind, the central focus of data privacy is social exposure, community belonging, and the deeply personal decision to acknowledge mental distress rather than complex questions in relation to date sharing. Where users are not convinced of the confidentiality of their shared personal information in technology- based mental health tools, engagement with such tools will naturally decline.

In Nigeria, it is more important to note that these cultural predispositions in relation to data privacy have affected the female gender who experience stigmatization during pregnancy-related mental health which in long run avoid clinical services, to patronize technological tools which provides less stigmatization, more confidentiality and anonymity.[84] This pattern illustrates a broader principle: in contexts where mental health stigma is severe and social consequences for disclosure are real, privacy is not a peripheral feature of a mental health app. It is central to whether the app functions at all as a meaningful access point for care.

6.3 Algorithmic Bias and the Perpetuation of Mental Health Stereotypes

Several scholars have noted how AI systems used for mental health screening may misidentify or underdiagnose distress when applied to populations outside their training distribution.[85] For instance, AI tools trained on data from high-income, Western contexts may fail to recognise the culturally specific ways in which Nigerians describe and experience depression, anxiety, or other mental health conditions. Natural language processing systems, which underpin many conversational mental health apps have been shown to produce performance disparities across racial, ethnic, and linguistic groups, and these disparities can translate into diagnostic errors or irrelevant therapeutic recommendations.[86]

---

80 F Oluwafemi and others, 'Barriers to the Use of Mental Health Services Amongst Men in Nigeria and the Potential of Digital Mental Health Support' (2023) 22(3) *Advances in Mental Health* 590-602

81 N Labinjo and others, 'Digital Mental Health: Integrating Psychotherapeutic Innovations and Technology — A Nigerian Perspective'(2025) 35(6) *Journal of Psychiatry and Allied Disciplines* 843–851.

82 A Ogunwale, B Fadipe and O Bifarin, 'Indigenous Mental Healthcare and Human Rights Abuses in Nigeria: The Role of Cultural Syntonicity and Stigmatization' (2023) *Frontiers in Public Health* (2023) 11:1122396

83 Labinjo and others (n 82)

84 L Kola and others, 'Factors Impacting Mobile Health Adoption for Depression Care and Support by Adolescent Mothers in Nigeria: Preliminary Focus Group Study'(2025) *JMIR Formative Research* PMC12018861

85 T Chaspari and others, 'AI for Mental Health Screening May Carry Biases Based on Gender, Race' (University of Colorado Boulder, 5 August 2024) <https://www.colorado.edu/today/2024/08/05/ai-mental-health-screening-may-carry-biases-based-gender-race> accessed 15 February 2025

86 D Yoffe and others, 'Racial Bias in AI-Mediated Psychiatric Diagnosis and Treatment: A

Beyond diagnostic accuracy, algorithmic bias poses a subtler but equally important risk which is the reinforcement of stigmatizing narratives about mental health in specific populations. When data collected by apps is used to build predictive models that associate race, language, or geographic location with particular mental health outcomes, those models can embed and amplify existing prejudices. An argument between Timmons and colleagues, writing in the journal Perspectives on Psychological Science, was premised on the fact that the bias in AI mental health tools is likely to increase as these systems become more widely deployed. [87] Hence, if there are no deliberate corrective measures, these tools risk perpetuating the very inequities that mental health technology is meant to address.[88]

In Nigeria specifically, these concerns become compounded with the absence of adequate regulatory framework governing AI applications in general.[89] The effect is that Nigerian users may be subjected to algorithmically bias mental health assessments without any regulatory mechanism to identify, challenge, or remedy those biases.

7. Comparative Analysis: User Rights and Trust

7.1 European Union

The European Union General Data Protection Regulation (GDPR) serves as the legal framework for the collection and processing of personal data within the European Union.[90] It replaced Directive 95/46/EC, which addressed the protection of individuals concerning personal data processing and the free movement of such data. [91] The GDPR was established to safeguard the privacy rights of EU residents, reflecting the EU's strong constitutional commitment to data protection. [92] This commitment has been described as deeply ingrained and central to the identity of the EU as an information-age political entity.[93] In the EU, privacy is considered a fundamental right that encompasses family life, reputation, and communications.[94] Article 8 of the Charter states that everyone has the right to the protection of personal data concerning them.[95] Such data must be processed fairly, for specified purposes, and based on the consent of the individual concerned or another legitimate basis established by law.[96] Everyone has the right to access and rectify their collected data.[97] Additionally, the Charter mandates that an independent authority oversees compliance with these rules.[98] The principles of the Nigeria Data Protection Act 2023 (NDPA) are similar to those of the GDPR, though there are some differences between the two. Both the NDPA 2023 and the GDPR provide similar definitions for terms such as 'processing,' 'personal data,' and 'sensitive personal data.' The definition of 'personal data' under the NDPA 2023 shares certain similarities with the definition provided in the GDPR.[99]

Qualitative Comparison of Four Large Language Models' Nature (2025) PMC12137607

87 AC Timmons and others, 'A Call to Action on Assessing and Mitigating Bias in Artificial Intelligence Applications for Mental Health' (2023) 18(5) Perspectives on Psychological Science 1062

88 Ibid.

89 Lionel Ebenibo and others, 'Evaluating the Sufficiency of the data protection act 2023 in the age of Artificial Intelligence (AI): A Comparative Case Study of Nigeria and the USA' (2024) I5(1) *Internationa*l *Journal of Scholarly Research and Reviews*:088-107

90 Came into operation in 2018 and is applicable in all member states of the European Union to harmonize data privacy laws across Europe. 'General Data Protection Regulation (GDPR) – Official Legal Text'<https://gdpr-info.eu/> accessed 22 March 2022

91 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

92 P. Sen, 'EU GDPR and Indian Data Protection Bill: A Comparative Study' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834112> accessed 22 March 2022; C. J. Hoofnagle, B. van der Slootand F. Z. Borgesius 'The European Union General Data Protection Regulation: What It is and What It Means' (2019) *Information & Communications Technology Law* 2. The EU Charter of Fundamental Rights and the EU Treaties both guarantee the right to privacy and the right to the protection of personal data

93 ibid, 2

94 Article 8 of the 1950 European Convention on Human Rights provides protection to private and family life, home, and communication. Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8, 4 November 1950, 213 U.N.T.S. 222

95 Charter of Fundamental Rights of the European Union (OJ C 364 of 18 December 2000) <https://www.europarl.europa.eu/charter/pdf/text_en.pdf> accessed 22 March 2022. Hereafter referred to as the Charter

96 The Charter, art 8(2)

97 ibid, art 8(2)

98 ibid, art 8(3)

99 NDPA 2023, s. 65. Under Article 4 of the General Data Protection Regulation (GDPR), personal data is defined as 'any information relating to an identified or identifiable natural person ('data

Data controllers and processors must adhere to the GDPR by incorporating policies and measures aligning with the data protection principles by design and default (DPbD).[100] GDPR's "privacy by design" and "privacy by default" principles are crucial for developing compliant digital health apps. This means prioritizing data protection throughout development and setting the strictest privacy settings as the default option.

DPbD, or Data Protection by Design, requires creators of products, services, and software used to handle personal data, including mental health apps, to prioritise data protection.[101] They must consider data protection rights when developing such products, services, and software. Additionally, they must ensure that those responsible for data processing can adhere to legal requirements, taking into account the latest technological advancements.[102] This is an integral part of being accountable and it involves integrating data protection throughout all activities and processing steps.[103] The GDPR makes recommendations for potential suitable actions, including data minimisation,[104] transparency[105] concerning the functions and processing of personal data, enabling the data subject to monitor the data processing, using pseudonymisation techniques,[106] and enhancing security features.[107] The process includes establishing protective measures at the outset of processing activities and during the processing itself, to uphold the data protection principles and preserve individual rights.[108] This method of safeguarding data is proactive rather than reactive, and it focuses on prevention rather than remedy.[109] A DPbD approach involves being proactive about data protection by anticipating privacy issues and risks, rather than waiting until breaches occur.[110]

The NDPA 2023 does not explicitly use the term "data protection by design and by default"; however, this approach is implicitly reflected and further operationalised under the GAID 2025. In particular, Article 31 GAID requires data controllers deploying software (including mobile applications) to implement privacy by design and by default, conduct a DPIA prior to deployment, and embed privacy policies and safeguards within the system architecture. However, data controllers are mandated by the NDPA 2023 to enforce suitable technical and organizational measures to safeguard the security, integrity, and confidentiality of personal data that they possess or control.[111] This includes implementing protections against accidental or unlawful destruction, loss, misuse, or access.[112] Some of the steps involve using pseudonyms, securing personal data through encryption, implementing procedures to guarantee the security, accuracy, privacy, accessibility, and robustness of processing systems and services, and more.[113]

Conducting Data Protection Impact Assessments (DPIAs) is crucial for implementing Data Protection by Design (DPbD).[114] The Data Protection Impact Assessment (DPIA) is a valuable tool for promoting accountability and enhancing the controller's responsibility.[115] The GDPR requires a Data Protection Impact Assessment (DPIA) when the data processing is likely to pose a significant risk to the rights and freedoms of individuals, especially when the data controller employs new technology for processing data.[116] Controllers are required to notify the supervisory authority if a high-risk data processing activity lacks risk-reduction measures, as per Article 36 of the GDPR.

Many digital health apps already require Data Protection Impact Assessments (DPIAs) under EU

subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.'

100 GDPR, recital 78

101 ibid

102 ibid

103 ICO, 'Guide to the General Data Protection Regulation' 157 <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed 28 May 2024

104 GDPR, art 5(1)(c)

105 Ibid, art 12–14

106 Ibid, art 25(1)

107 Ibid art 32, recital 78

108 ICO, 'Guide to the General Data Protection Regulation' (n.)179

109 ibid

110 ibid

111 NDPA 2023, s.49(1)

112 ibid

113 ibid, s.40(2)

114 ICO, 'Guide to the General Data Protection Regulation' (n.) 182

115 K. Demetzou,'Data Protection Impact Assessment: A tool for Accountability and the Unclarified Concept of "High Risk" in the General Data Protection Regulation' (2019) *Computer Law & Security Review* 3.

116 GDPR, art. 35(1)

regulations.[117] These assessments help pinpoint potential risks to users' privacy when processing their information.[118] By identifying these risks early, developers can find user-friendly solutions to mitigate them.[119] DPIAs are crucial for two reasons.[120] Firstly, they fulfil the GDPR's requirement for organizations to be accountable for data protection practices.[121] Secondly, they demonstrate an app's compliance with GDPR and they should be documented and reviewed regularly. Since digital health apps often handle health data, considered 'special categories of personal data' under GDPR, processing this information must strictly adhere to Article 9, paragraph 2 of the regulation.[122]

Notably, the NDPA 2023 makes provision for circumstances where a data controller is to carry out a DPIA.[123] This obligation is significantly elaborated under Article 28 of the GAID 2025, which mandates DPIAs for high-risk processing activities, including healthcare services, sensitive personal data processing, and the deployment of digital applications such as mental health apps. This has several implications for Nigeria, for instance, DPIAs can help developers identify vulnerabilities in their apps that could lead to leaks of sensitive mental health data.[124]

By addressing these weaknesses before launch, the risk of exposing users' private information is minimised.[125] The DPIA process encourages developers to be more transparent about how they collect, use, and store mental health data. This transparency can build trust with users who might be hesitant to share sensitive information.[126] DPIAs can also help developers identify features or functionalities within the app that might pose privacy risks. This allows them to design the app in a way that protects user privacy while still offering valuable mental health services.

The NDPA does not currently specify how DPIAs should be conducted for mental health data specifically. The Nigerian Data Protection Commission will need to provide clear guidelines to ensure developers understand how to assess the unique risks associated with this type of data. Conducting DPIAs requires time and expertise. Smaller app developers might struggle to dedicate the resources necessary for a thorough assessment, especially if the requirements are complex. As with the overall NDPA, the effectiveness of DPIAs for mental health apps hinges on strong enforcement mechanisms. Clear penalties for non-compliance will be essential to ensure developers take DPIAs seriously.

Under the GDPR, digital mental health apps typically need users' explicit consent to process their health information.[127] This is because health data is classified as 'special' due to its sensitive nature. For situations beyond basic processing, such as using the data for research purposes, additional legal justifications might be required on top of consent.[128] Notably, the situation is the same in Nigeria, as health data is classified as 'sensitive personal data,'[129] this is reinforced under Article 18 of the GAID 2025. Processing of such data also requires the explicit consent of the data subject.[130]

Both the GDPR and the NDPA 2023 emphasize a key principle: data collected for a specific purpose cannot be reused for something entirely different and unrelated.[131] The NDPA and GDPR both require transparency. If one intends to utilize the information acquired from the application for purposes extending beyond its fundamental functionality, such as contributing the data for research or employing it for product development, it is imperative to transparently disclose this intention from the outset.[132] Clarity regarding all envisaged uses is essential, and it is crucial to ensure the presence of a valid legal basis for each use, such as user consent, at the time of data collection.

Worthy of note is Articles 13 and 14 of the GDPR, which emphasise transparency and the need for data subjects to understand how their personal data is used. Data controllers must describe data processing in the privacy policy in a way that is clear, specific to the

117 Schwarz, (n 78)
118 Ibid
119 ibid
120 ibid
121 GDPR, art. 5(2)
122 Schwarz, (n 78).
123 NDPA 2023, s.28
124 For the different phases of a DPIA, see M. Friedewald and others 'Data Protection Impact Assessments in Practice' In S. Katsikas, and others *Computer Security* ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science, 13106. (Springer,2022) 428.
125 G. G. Várkonyi and A. Gradišek, 'Data Protection Impact Assessment Case Study for a Research Project Using Artificial Intelligence on Patient Data' (2020) 44 *Informatica* (2020) 497–505.
126 Ibid, 498
127 GDPR, art. 9(2) (a)
128 Ibid, art.9 (2) (j)
129 NDPA 2023, s.65
130 Ibid, s.30
131 GDPR, art.5 (1) (b), NDPA 2023, s.24 (1) (b)
132 Schwarz, (n 78).

app's functionalities, and easy for users to understand.[133] They must also provide a privacy policy early and right when personal data is collected from the user.[134] This typically means including it on the app download platform (e.g., app store) and during initial app access.[135] In addition to the download platform, make sure the privacy policy is readily available within the app. Users should be able to find it easily at any time.[136] These requirements are broadly reflected in Nigeria under Article 27 of the GAID 2025, although the GAID does not prescribe detailed usability or readability standards for privacy notices.

Some digital health apps choose a decentralized approach, whereby the personal data collected remains on the user's device.[137] The data is therefore not hosted externally (via server or cloud), which at the same time significantly reduces the risk of misuse.[138] A decentralized approach also strengthens user trust in a privacy-friendly and abuse-proof infrastructure of the respective digital health app.[139] If, on the other hand, it is necessary to store the data collectively on a server/cloud, the data must be transmitted and stored in sufficiently encrypted form to ensure data security.[140] However, when storing data collectively on a server or cloud is necessary, robust security measures become crucial.[141] Encryption plays a key role here. By ensuring data is transmitted and stored in a sufficiently encrypted form, these apps demonstrate a commitment to data security. This strong security posture translates to greater user confidence and trust in the app's infrastructure.

The recent trends within the European Union (EU) with regard to digital health technologies and intensive use of data have greatly enhanced the scope of the GDPR model. Regulation (EU) 2024/1689 or the Artificial Intelligence Act (AI Act) provides a risk-based regulatory framework for artificial intelligence systems.[142] Article 6 and Annex III classify AI systems in healthcare applications, such as emergency triage and medical device software, as "high-risk" systems. In this regard, such systems shall be governed by stringent legal requirements that include the establishment of a risk management system,[143] strong data governance and management practices,[144] and transparent user information.[145] Moreover, appropriate human supervision[146] and post-market surveillance[147] are mandatory requirements for providers of high-risk AI systems. These obligations complement the GDPR, emphasising key GDPR principles as accountability and privacy by design by implementing them throughout the process of development of AI systems.[148]

Concurrently, the European Health Data Space (EHDS)[149] is an important development in terms of sector-specific efforts to achieve consistency in how health data are used, accessed, and shared within the EU. In particular, the EHDS aims to enable primary and secondary uses of health data, while ensuring that strict protections for data subjects remain in place.[150] New governance arrangements, interoperability, and rights over electronic health data are some of the features of the EHDS.[151]

These measures combined point to a wider regulatory trend in the EU, which includes sectoral and technological specialization in highly sensitive sectors like digital health and mental health solutions. The EU's approach to regulation does not only consider its overarching general data protection principles but increasingly involves the development of multiple

133 Ibid.
134 Ibid.
135 Ibid.
136 Ibid.
137 Ibid.
138 Ibid.
139 Ibid.
140 Ibid.
141 ibid.
142 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024/1689.
143 Ibid, art 9
144 Ibid, art 10
145 Ibid, art 13
146 Ibid, art 14
147 Ibid, art 61
148 M Veale, and F Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act: Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' . (2021) 22(4) *Computer Law Review International*, 97–112.
149 Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. (2025). *Official Journal of the European Union*, L series, 2025/327. http://data.europa.eu/eli/reg/2025/327/oj
150 Ibid art 4
151 S Kalkman, 'Responsible Data Sharing in International Health Research: The European Health Data Space' (2023) 30(12) *European Journal of Human Genetics*, *30*(12), 1344–1350; M Shabani, 'The European Health Data Space: A New Paradigm for Health Data Governance' (2023) *Health Policy*, *135*, 104861.

layers of regulations, with the GDPR serving as one layer, complemented by specific measures that address the unique risks of new technologies. This phenomenon is consistent with the concept of "regulatory densification" or "normative layering" whereby multiple legal instruments interact to create a more robust and context-sensitive system of data governance[152]

7.2 South Africa

The Nigeria Data Protection Regulation (NDPA 2023) forms the basis of data protection in Nigeria, while the Protection of Personal Information Act (POPIA 2013) and the National Health Act 2003 form the basis of data protection in South Africa. Some notable differences emerge from a comparative analysis of the laws on the subject in both countries.

In South Africa, the right to privacy is guaranteed in Section 14 of the Constitution of the Republic of South Africa 1996.[153] The right is not so different from that of Nigeria. This right is however limited by Section 36 of the Constitution of South Africa which provides that such right may be limited to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality, and freedom considering key factors, including the nature of the right, the importance of the purpose of the limitation, the nature and extent of the limitation, the relation between the limitation and its purpose, and less restrictive means to achieve the purpose. It is commendable that the South African Constitution requires the use of the less restrictive means to achieve the purpose. Thus, in line with this provision, a judge may approve, order the termination, or take any other appropriate action in respect of an interference with the right to privacy only after determining whether the interference is legal, necessary, and proportionate.

The primary law on data protection in South Africa is the Protection of Personal Information Act, 2013 (POPIA Act),[154] which specifies the minimum requirements for accessing and processing personal information. Under the Act, the Information Regulator, a data protection authority is established to ensure that the principles of the POPIA Act are complied with.[155] The POPIA Act emphasizes that the Information Regulator should be independent and subject only to the Constitution and the law and must be impartial to perform its duties and exercise its powers without fear, favour, or prejudice.[156] The Independent Regulator is accountable to the National Assembly.[157]

In South Africa, Health information is classified as "special personal information" according to Section 26(1) (a) of POPIA and thus receives special protection. However, if the data are anonymised to prevent re-identification, they are excluded from the scope of POPIA. Section 26 prohibits the processing of special personal data which includes health data. However, Section 32 of the POPIA deals with exceptions to this rule. It has been argued that this provision might allow health data collected through apps to be shared with medical insurers or HCPs under specific circumstances.[158]

In South Africa, Section 14 of the National Health Act 2003 protects a wide range of user information, including details about a user's health status, treatment, and stay in a health establishment.[159] This aligns with the sensitive nature of data collected by mental health apps. The default position is confidentiality, meaning user information cannot be disclosed without consent.[160] This is crucial for protecting user privacy in mental health apps, where users might be hesitant to share information if they fear it will be revealed. The default position is confidentiality, meaning user information cannot be disclosed without consent. This is crucial for

---

152 A de Streel, 'The EU Digital Regulatory Framework: A New Model' (2022) 13(3) *Journal of European Competition Law & Practice*, 163–165; L Floridi, and others, 'AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' *Minds and Machines*, (2018). *28*(4), 689–707.

153 <https://www.gov.za/documents/constitution/constitution-republic-south-africa-1996-1> accessed 12 January 2021

154 Protection of Personal Information Government Gazette Republic of South Africa Vol. 581 No. 4 2013 <https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf> accessed 9 December 2022

155 POPIA 2013, s.39 and s.40

156 POPIA Act 2013, s.39 (b) and (c)

157 ibid, s.39(d)

158 D. Brand and others, 'What Constitutes Adequate Legal Protection for the Collection, Use and Sharing of Mobility and Location Data in Health Care in South Africa?' (2023) 119(5-6): S Afr J Sci., 14605, \\<https://pmc.ncbi.nlm.nih.gov/articles/PMC11210507/> accessed 8 May 2026

159 National Health Act, 2004, No 61 of 2003, available at https://www.gov.za/sites/default/files/gcis_document/201409/a61-03.pdf accessed 6 June 2024

160 Ibid, s.14(2) (a)

protecting user privacy in mental health apps, where users might be hesitant to share information if they fear it will be revealed. Disclosures are permitted under certain circumstances, including with user consent, court orders, or threats to public health.[161] While these exceptions are reasonable, they create situations where confidentiality might be compromised. It is commendable that disclosure of user information by healthcare providers is permitted only for legitimate purposes within the scope of their duties and when it is in the user's best interests.[162] This ensures information is used responsibly and for providing care. However, the law does not define "legitimate purpose" precisely. This could lead to interpretations that allow for broader data sharing than intended, potentially affecting user privacy in mental health apps. This law provides a foundation for data privacy in mental health apps in South Africa. However, the exceptions and lack of specific definitions leave room for improvement.

Moreover, it has been argued that low literacy levels in some South African communities make it challenging for users to understand consent and data sharing practices in apps.[163] A recent study has highlighted the importance of data protection for health information collected through mobile apps in South Africa.[164] It emphasized the need for clear user consent, responsible data sharing practices, and specific considerations for vulnerable populations like children.[165] While South Africa lacks specific mobile app guidelines, the EU's "Guidelines on Mobile App Data Protection" offer helpful principles for lawful data processing.[166]

A few lessons Nigeria can learn from South Africa are discussed below:

South Africa has gone past data protection at large to health-specific guidelines. In 2026, the Information Regulator promulgated the Regulations on the Processing of Health Information.[167] The Regulations explain precisely how to process such information for all stakeholders involved including the insurance companies, employers, and medical schemes. The purpose of the Regulations include: to assist responsible parties in the correct interpretation of section 32(6) of the Act; provide more transparency to data subjects about how their health information may be used and provide a framework to the Information Regulator to enforce mechanism for processing health information of data subjects as provided in section 32(6) of the Act.[168]

Broad laws like the NDPA leave mental health app developers in “gray area.” Nigeria should emulate South Africa and develop specific subsidiary legislation or a “Code of Conduct” for digital health. This would give specific technical standards for encryption and anonymisation which general law lacks.

The South African legal system is heavily dependent on the constitutional “limitation clause.”[169] The South African Model: Any processing of sensitive data that infringes privacy must satisfy a three-part test: Is it lawful, necessary, and is there a way to accomplish the goal with less restriction? Nigeria’s NDPA allows processing on the basis of “legitimate interest”. But without a hard proportionality test, this can become a loophole for invasive data collection. If app developers were to adopt the South African approach of “least restrictive means”, they would be required to limit data collection to the absolute minimum required for therapy.

The need for transparent and user-friendly privacy policies is clear, such as Articles 13 and 14 of the GDPR, which calls for app-specific, accessible disclosures provided at the point of data collection and perpetually available within the application. The NDPA 2023, implemented by the GAID 2025, incorporates similar principles, such as privacy by design and by default, the requirement for explicit consent for sensitive personal data, mandatory Data Privacy Impact Assessments for high-risk processing activities like the provision of healthcare services, and in-app privacy notices. However, the practical impact of these safeguards varies across jurisdictions. In the EU these obligations are embedded in a well-developed enforcement ecosystem with established regulatory practices and meaningful penalties for non-compliance.

161 Ibid, s.15
162 Ibid.
163 Brand, and others, (n 159).
164 Ibid.
165 Ibid.
166 Ibid, 4
167 Regulations Relating to the Processing of Data Subjects' Health Information by Certain Responsible Parties, 2026 Government Notice 7198 of 2026 https://lawlibrary.org.za/akn/za/act/gn/2026/7198/eng@2026-03-06
168 Ibid, chapter 2
169 POPIA s 36

This makes an important difference for user. EU citizens use mental health apps in a developed regulatory regime where compliance measures such as obtaining explicit consent, providing adequate privacy notices, and performing data protection impact assessments are not only necessary but are also commonly enforced. This is also the case for Nigeria under NDPA 2023 and GAID 2025 (Articles 18 and 28), which require explicit consent for processing personal data and make DPIA mandatory for high-risk data processing activities. The effectiveness of these mechanisms is dependent on the growing expertise of the Nigerian Data Protection Commission.This asymmetry in effective protection, rather than formal rights, is what shapes user trust in practice.[170]

Adapting aspects of the GDPR framework to strengthen Nigerian mental health app regulation holds considerable promise, though it must be approached with an understanding of Nigeria's specific legal, socioeconomic, and cultural context. The GDPR's "data protection by design" principle, which requires privacy safeguards to be embedded into systems from the earliest stages of development, is directly applicable to the Nigerian mental health app sector and has been mandated through sector-specific guidelines issued by the Nigeria Data Protection Commission under its existing statutory authority. There is the General Application and Implementation Directive (GAID) 2025, which requires data controllers to prioritise privacy-by-design and by default.[171] Similarly, although the GDPR's Data Protection Impact Assessment requirement is mirrored in the NDPA 2023, Article 28 of the GAID 2025 goes further by expressly mandating DPIAs for high-risk processing, including healthcare services and sensitive data; however, more explicit, sector-specific guidance for mental health applications may still be necessary to address their unique risks.

GDPR Articles 13 and 14 set the standard for transparency, but such principles are already included within GAID 2025, specifically Article 27, which mandates that information must be clear, accessible, and comprehensible, especially to vulnerable data subjects and Article 7, which mandates that privacy policies must be published on appropriate channels. However, such principles are yet vague, as they do not set out concrete criteria for comprehension. Hence, the issue of compliance privacy policies indicates a gap not in legal recognition but in the operationalisation and enforcement of plain-language transparency.

As illustrated above, there exists a practical relationship between the regulation of data privacy and mental health. Data privacy regulations are not neutral technical instruments; they define the environment that affects people's decision to seek help, expose weaknesses, and make use of technological innovations that aim to improve their lives. In a country like Nigeria, where mental health facilities are scarce and there is still a significant level of stigma surrounding mental disorders, the effectiveness of mental health applications hinges on the effectiveness of their data privacy regulations. Failure to ensure proper data privacy will translate to non-use of the application and hence the inability to derive any benefits from it.

The comparative analysis demonstrates that both the GDPR and the NDPA 2023 share the same fundamental objectives of data subject rights protection, limitation of data usage for particular reasons, and increased regulation regarding the processing of sensitive personal information. Their differences include the level of advancement in the enforcement process, the extent of the regulations provided, and the presence or absence of provisions concerning the mental health sector as a context with a higher risk. The GDPR has been elaborated over years and has evolved due to regulatory guidance by national data protection authorities and the European Data Protection Board. In turn, while Nigeria is developing a compliance expectation environment, its plan of legislative initiatives cannot be called insufficiently ambitious. This idea can be supported by POPIA's experience in South Africa. Indeed, formal alignment of laws with international data protection standards is important, but not sufficient.[172]

From a mental health standpoint, the results of this study corroborate the long-held understanding among clinical practitioners and public health researchers that trust holds therapeutic significance.[173] Patients or

[170] International and Comparative Law Guides, 'Data Protection Laws and Regulations Report 2025–2026: Nigeria' ICLG (2025) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria> accessed 15 February 2026

[171] GAID 2025, art 26 and 28(11)

[172] S Mishi and G Anakpo, 'Regulatory Challenges of Digital Health: The Case of Mental Health Applications and Personal Data in South Africa' (2025) *Frontiers in Digital Health* PMC12074941

[173] CIHI, 'Trust is Essential to Public Health's Success' (April 16, 2026) <https://www.cihi.ca/en/priority-indicators-for-public-health-systems-in-canada/foundations-of-public-health-systems/trust> accessed 8 May 2026

prospective patients who lack confidence in the protection of their disclosures tends to withhold information, withdraw from care, and cope with their distress privately, frequently in maladaptive ways. In the realm of mental health applications, the data privacy framework does not serve as an administrative backdrop to the therapeutic interaction. For many Nigerian users, it is the main factor that decides if any kind of therapy will happen.

8. Recommendations

On the basis of this analysis, the following recommendations are offered to policymakers, app developers, and the mental health community in Nigeria:

First, there should be a regulation that expressly covers mental health data collected and processed through digital platforms, including mobile applications. As presently constituted, the National Health Act's confidentiality protections apply to health establishments and their personnel; they do not extend to third-party app developers who may process equally sensitive mental health information without any clinical relationship with the user. Closing this gap would ensure that the therapeutic confidentiality expectations users bring to mental health apps are mirrored in the legal framework that governs them.

Second, app developers operating in the Nigerian mental health space should adopt a privacy-by-design approach as a matter of ethical best practice and commercial necessity. In other words, the issue of user privacy must be thought through in advance as part of the design of the app itself, rather than being implemented later just to satisfy legal requirements. More specifically, this includes giving users precise control over the collection of their data, keeping data decentralized where possible to decrease vulnerabilities, conducting periodic third-party security audits, and providing easily understandable privacy policy information, including a detailed description of the data that is collected, how this data is used, and which entities have access to this information. Moreover, developers need to disclose any algorithmic decision-making process used and allow for challenges to those decisions affecting care.

Third, there needs to be an active partnership between the Nigeria Data Protection Commission, the Federal Ministry of Health, organizations representing mental health professionals such as the Association of Psychiatrists of Nigeria, and the tech industry on creating an ethical framework for AI applications in mental health care. This framework will include provisions for monitoring algorithmic bias, cultural competence of AI mental health solutions, and basic clinical safety requirements.

Fourth, culturally sensitive public education campaigns should be carried by the government and private bodies to address the intersection between mental health stigma and concerns about digital privacy. Such campaigns should explain in accessible language the mental health benefits of digital support tools, as well as the legal protections that exist for users' data. They should be designed with an awareness of Nigeria's ethnic, linguistic and religious diversity and delivered through community channels including faith-based organisations, universities and local radio that have established credibility with target populations. Addressing stigma and promoting privacy literacy are two sides of the same coin. When users who clearly understand their rights and believe those rights will be protected, they are more likely to use mental health tech in ways that genuinely support their wellbeing.

9. Conclusion

This paper examined the link between the data privacy practices of Nigerian mental health apps and the existing legal frameworks. It compared Nigeria's regulatory environment with the GDPR and South Africa's POPIA. What this analysis indicates is not just a technical assessment of regulatory gaps, but a human rights argument: where data privacy protections are inadequate, the ability of vulnerable individuals to access mental health care is correspondingly diminished. The stakes here are not just commercial and administrative in terms of data privacy. They are clinical and urgent at a time when the country is grappling with a mental health crisis of enormous dimensions.

Nigeria is at a crossroads. The Nigeria Data Protection Act 2023 is a true legislative landmark, a principled comprehensive framework, appropriately drawing on international best practice, and establishing an independent regulatory body with meaningful enforcement powers. The private sector is beginning to respond to unmet demand, as evidenced by the country's growing digital health ecosystem, which has witnessed the emergence of AI-powered mental health platforms tailored to African users. And the signing of the National Mental Health Act in January 2023 indicates that the policy makers get the scale of the mental health challenge. What remains, however, is the work of implementation: translating legislative intent into effective protection, and effective

protection into the user trust upon which digital mental health adoption ultimately depends.

The lessons from the GDPR and POPIA are valuable but cannot be directly transplanted to Nigeria. The regulatory path should be informed by Nigeria's social and economic context, and its rich cultural and linguistic diversity. Other factors include high levels of stigma around mental health, and limits on regulatory capacity. The European and South African experiences do not offer a strict template but do highlight important principles such as privacy by design, mandatory impact assessments, clear transparency, meaningful consent and effective enforcement. The challenge before Nigerian policy makers, regulators and civil society is to adapt these principles quickly, correctly and with a clear understanding of the communities they serve.

This paper suggests a number of directions for future research. For example, there is a lack of data on the privacy perceptions of Nigerian users of mental health apps. The body of evidence will be significantly strengthened by studies that give priority to the voices and experiences of these users and consider factors such as gender, age, socioeconomic status and geographic location. Specific app evaluations in Nigeria's legal compliance market and their actual data practices would provide regulators with the granular accountability information necessary to target their enforcement efforts. Research on how culturally adapted privacy communication strategies can build user trust is also equally important; it would help implement the recommendations in this paper.

Ultimately, findings of this study indicate the great potential of technology in improving access to mental health care in Nigeria. Digital platforms can help in reaching those without access – especially youth in remote areas – and providing mental health professionals with private avenues for self-care. These interventions are technologically feasible and provide a practical way to address the widespread treatment gap affecting millions across the country. However, it is important to emphasise the successful implementation of these benefits is fundamentally dependent on the establishment of user trust. However, in this scenario, the issue of trust does not relate to mere intentionality on the part of the developers alone; instead, it is based on the existence of an effective legal framework that protects the privacy of such mental health records, with adequate regulations and a society that views mental health care as a basic right.