White Paper on

Electronic Health Records

Policy Alignment Perspective

The Future of Electronic Health Records in Nigeria

By Kasim Sodangi, A

www.apiintelligence.org

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

01 UHC Universal Health Care

02 EMR Electronic Health Records

03 NHMIS National Health Management Information System

04 NITDA National Information Technology and Development Agency

05 NDPR Nigeria Data Protection Regulation

06 DPIF Data Protection Implementation Framework

07 CNII Critical National Information Infrastructure

08 NDPA Nigeria Data Protection Act

Executive Summary

Integrating technology into healthcare practices is indispensable in enhancing the delivery of healthcare services and realising the goal of Universal Health Care (UHC). Electronic Health Records (EHRs) have emerged as a crucial component in this digital transformation, replacing traditional paper-based systems and offering a centralised platform for securely storing, accessing, and managing patient data. Despite these benefits, challenges such as interoperability, data security, privacy concerns, and disparities in access to technology persist, hindering the seamless functioning of health information systems.

Addressing these challenges requires concerted effort from healthcare stakeholders, policymakers, technology developers, and the healthcare community. Initiatives to enhance data interoperability, implement robust data governance frameworks, and invest in cybersecurity measures are essential to fortifying the health information system. However, an aspect that often gets overlooked is digital literacy. Promoting digital literacy among healthcare practitioners and the public is not just a necessity but a powerful tool that empowers individuals and improves the quality of the healthcare system. Additionally, fostering collaboration and partnerships among various stakeholders can facilitate developing and implementing innovative solutions tailored to the specific needs and contexts of different healthcare environments.

In Nigeria, while existing legal frameworks such as the National Health Act of 2014, Nigeria Data Protection Regulation (NDPR) 2019, and the Data Protection Act 2023 provide some level of protection for health records, there remains a lack of a comprehensive framework specifically tailored for electronic health records (EHRs). Recognising this gap, the Nigerian legislature introduced the Electronic Health Record Bill in 2019. This bill, if passed, will establish a robust operational and managerial framework for digitising health records nationwide, enhancing data interoperability, implementing robust data governance frameworks, investing in cybersecurity measures, and promoting digital literacy. Unfortunately, the bill has not progressed to becoming law.

Moving forward, policymakers must prioritise the passage of comprehensive legislation specifically addressing electronic health records (EHRs) in Nigeria. This legislation, with its clear standards for protecting, storing, and transferring health data and provisions for breach reporting and user notification, holds the potential to transform the healthcare landscape. Sensitisation efforts targeting healthcare practitioners and the public on privacy and security implications are also urgently needed. Additionally, proactive measures such as prioritising application and network security, implementing robust encryption measures, and adhering to best security practices are essential to safeguarding the privacy and security of healthcare data. The potential benefits of this legislation are vast, offering hope for a more secure and efficient healthcare system in Nigeria.

Introduction

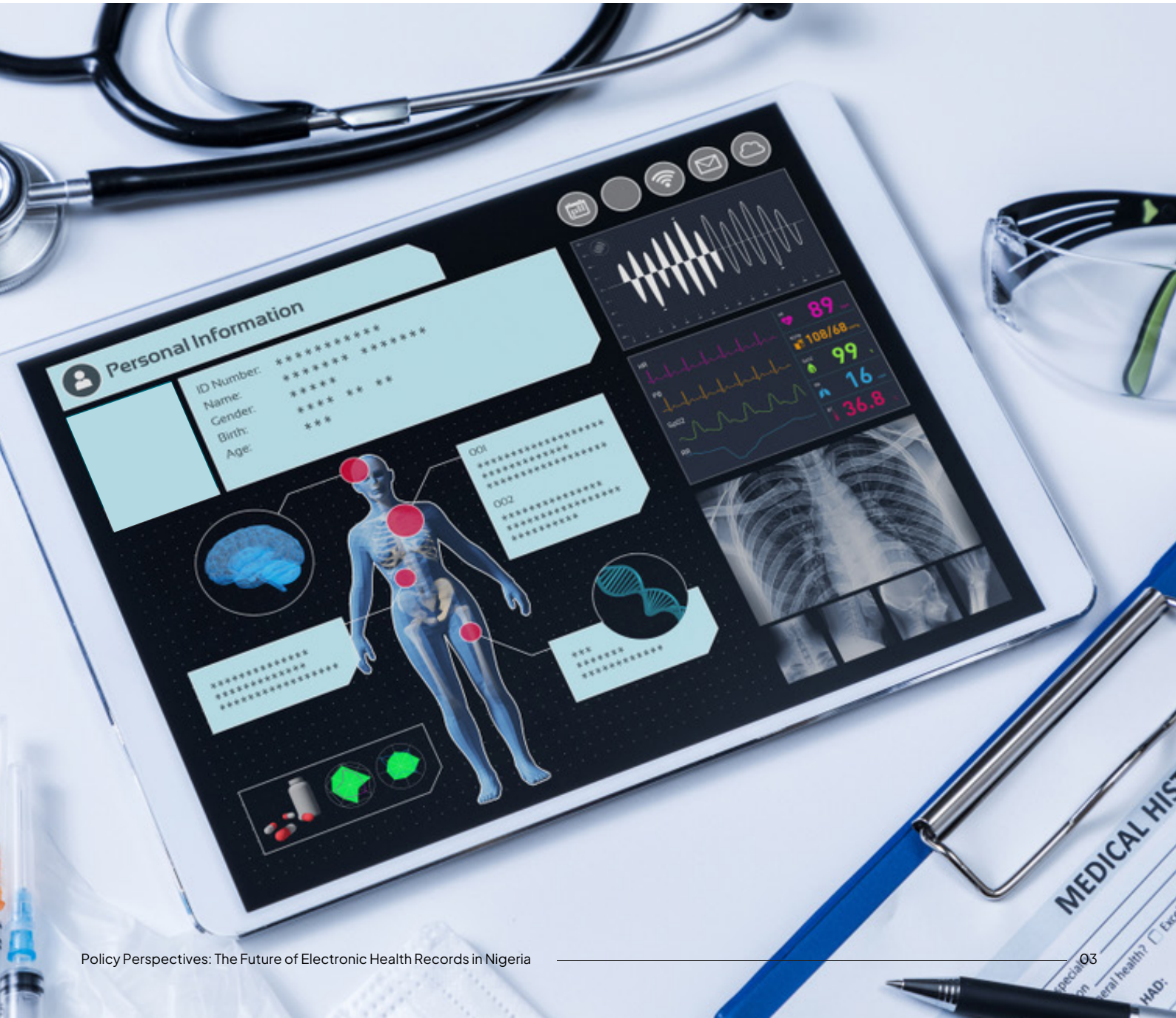
Adopting electronic health records is essential to digitising and adopting technologies in the health sector. Electronic health records (EHRs) are any digital document or system that contains information on an individual's health and care. This could be online, on an internal network, or a device.[1] It also involves the systems being defined as an electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorised clinicians and staff within one healthcare organisation that has the potential to provide substantial benefits to physicians, clinic practices, and health care organisations. These systems can facilitate workflow and improve the quality of patient care and patient safety.[2]

Adopting electronic medical records (EMRs) has improved physicians' access to comprehensive patient information. Patient vital data includes diagnoses, allergies, medical history, diagnoses, medications, treatment plans, immunisation dates, radiology images, and laboratory and test results. EMRs enable seamless retrieval of current and historical test results from various care settings and providers, fostering continuity of care. Furthermore, implementing computerised provider order entry systems has standardised healthcare orders, while computerised decision-support systems help mitigate drug interactions and improve adherence to best practices. Secure electronic communication channels facilitate interaction among providers and between providers and patients, enhancing care coordination. Additionally, patients are empowered through access to their health records and relevant health information resources. Automation of administrative tasks, such as scheduling systems, boosts operational efficiency, while the utilisation of standards-based electronic data storage and reporting mechanisms bolster patient safety initiatives and disease surveillance efforts.[3]

Despite these benefits, electronic medical records (EMRs) face several challenges in their widespread adoption and effective implementation within healthcare systems in Nigeria. These challenges include privacy and security concerns, with the risk of data breaches and unauthorised access to sensitive patient information being ever-present threats. Interoperability is another issue, as EMRs from different vendors often use proprietary formats and standards, hindering seamless data exchange between systems and healthcare providers. Additionally, the upfront costs of implementing EMR systems and ongoing maintenance expenses can pose financial barriers for healthcare organisations, notably smaller practices. Furthermore, resistance to change among healthcare professionals and the need for extensive training and workflow adjustments can impede the smooth integration of EMRs into clinical practice. Addressing these challenges requires concerted efforts to establish interoperability standards, enhance data security measures, provide adequate financial support and incentives, and offer comprehensive training and support to healthcare providers transitioning to EMRs.

[1] African Health Organisation.Electronic Health Records.
https://aho.org/programmes/electronic-health-records/
[2] Digital Healthcare Research Archive.. Electronic Medical Record Systems
https://digital.ahrq.gov/electronic-medical-record-systems
[3] Digital Healthcare Research Archive.. Electronic Medical Record Systems
https://digital.ahrq.gov/electronic-medical-record-systems

In Nigeria, the legal framework governing health records, primarily outlined in the National Health Act of 2014, emphasises data protection and delineates procedures for accessing and maintaining the confidentiality of health information. The Act also highlights the coordination of the National Health Management Information System (NHMIS) under the Federal Ministry of Health. The NHMIS ensures seamless data management, particularly in electronic health records (EHRs). The Nigeria Data Protection Regulation (NDPR) adopted by NITDA in 2019 and the subsequent Data Protection Act of 2023 further strengthened data protection measures, including those for health records. Despite these legal frameworks, there's a lack of a comprehensive framework specifically tailored for electronic health records (EHRs) in Nigeria. The Electronic Health Record Bill was introduced in 2019 to address this gap, aiming to establish a robust framework for digitising health records nationwide. Although the bill includes provisions for the National Electronic Health Record System and related operational structures, it is yet to become law. This whitepaper shifts focus to providing policy perspectives on the future of EHRs in Nigeria, acknowledging the need for comprehensive legislation in this domain.



The Current Nigerian Electronic Medical Record Landscape

The Nigerian government is actively pursuing the implementation of a National Electronic Health Record System (NEHR) as a cornerstone of its healthcare reform efforts. Policy documents such as the National Health Policy and the National Health ICT Strategic Framework 2015-2020 emphasise the importance of electronic health records (EHRs) in advancing healthcare delivery. Research conducted by the Federal Ministry of Health in 2017 revealed widespread use of electronic medical records in Nigeria. Recognising the critical role of health records in delivering quality care, public and private stakeholders are urged to embrace EHR systems. Inspired by similar

initiatives in other countries, the Nigerian House of Representatives introduced a Bill in 2019 to establish the NEHR system. The NEHR will be a secure platform for aggregating summary health records from various healthcare providers, allowing authorised professionals to access comprehensive patient information. Participation in the NEHR is voluntary, allowing citizens to securely store their health records in one centralised location. This facilitates seamless collaboration among healthcare professionals nationwide, enabling real-time access to patient data and improving the quality of care provided.

Case Examples of Breach of personal information in the health sector

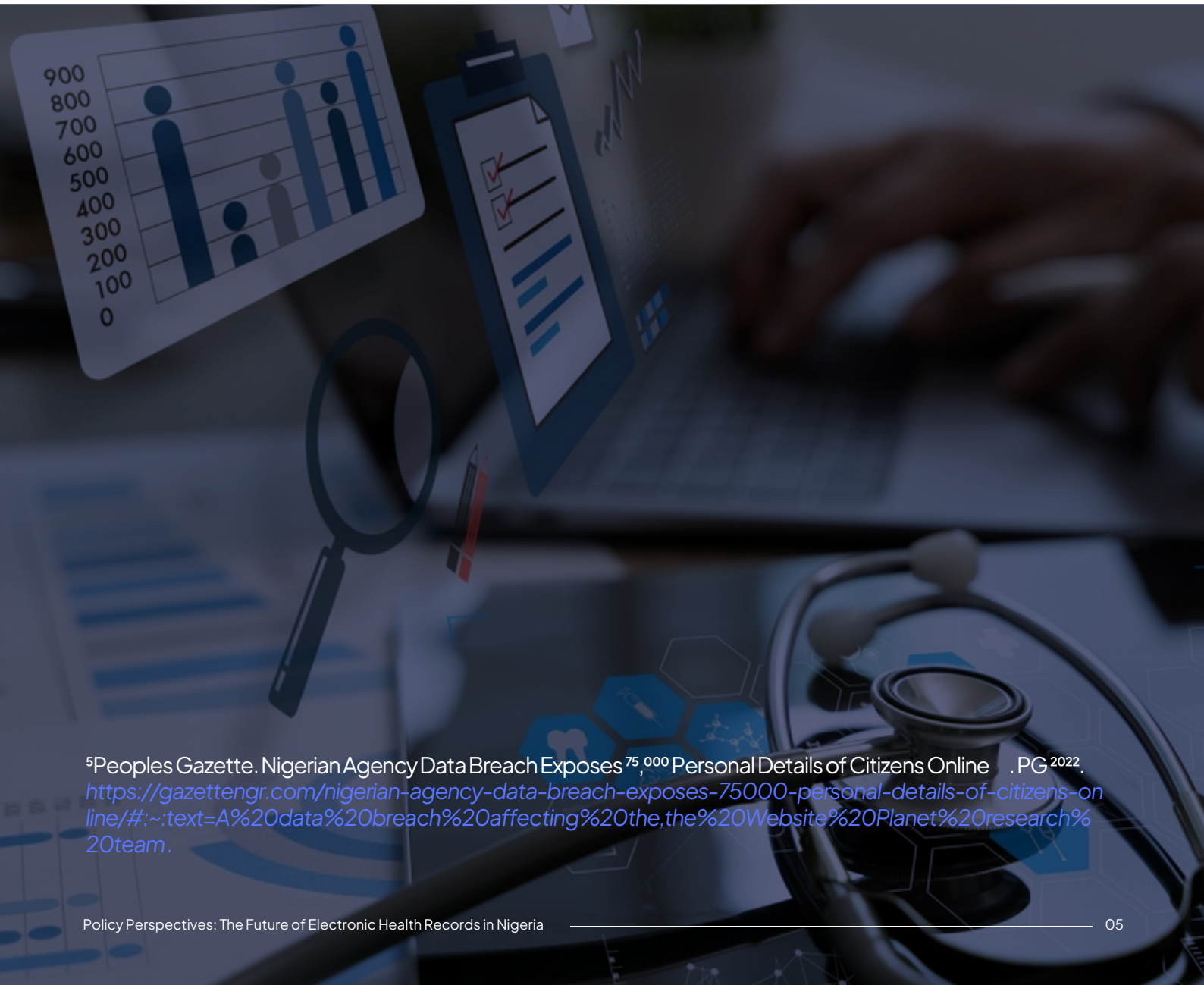
Data Breach Impacting Participants of Nigeria HIV/AIDS Indicator and Impact Survey (NAIIS) 2018

Recent findings have brought to light a significant data breach affecting roughly 80,000 individuals who participated in the Nigeria HIV/AIDS Indicator and Impact Survey (NAIIS) in 2018. Wizcase, a cybersecurity firm, detected vulnerabilities within the database servers of numerous medical websites globally. These servers were discovered to have insufficient security measures, allowing unauthorised access without password authentication. Consequently, millions of patients and medical personnel face potential exposure to privacy breaches. The impact of this breach extends beyond Nigeria, affecting countries such as Saudi Arabia, Brazil, Canada, China, the United States and France. The breach compromised sensitive data, including facility and hospital names, patients' pregnancy status, laboratory results, patients' ages, HIV validation first test dates and times, HIV encounter data, and medical observations of anonymous survey participants[4]. The survey targeted approximately 168,100 participants across Nigeria, spanning ages 0-64 years. With the unsecured NAIIS database totalling approximately one gigabyte, the breach poses a significant threat to individual privacy and data security. Urgent action is required from relevant companies and authorities to address these vulnerabilities and safeguard patient confidentiality.

[4]https://www.cybersecfill.com/protect-health-information-of-nigerian-citizens-a-case-of-nigeria-hiv-aids-indicat or-and-impact-survey-data-breach/

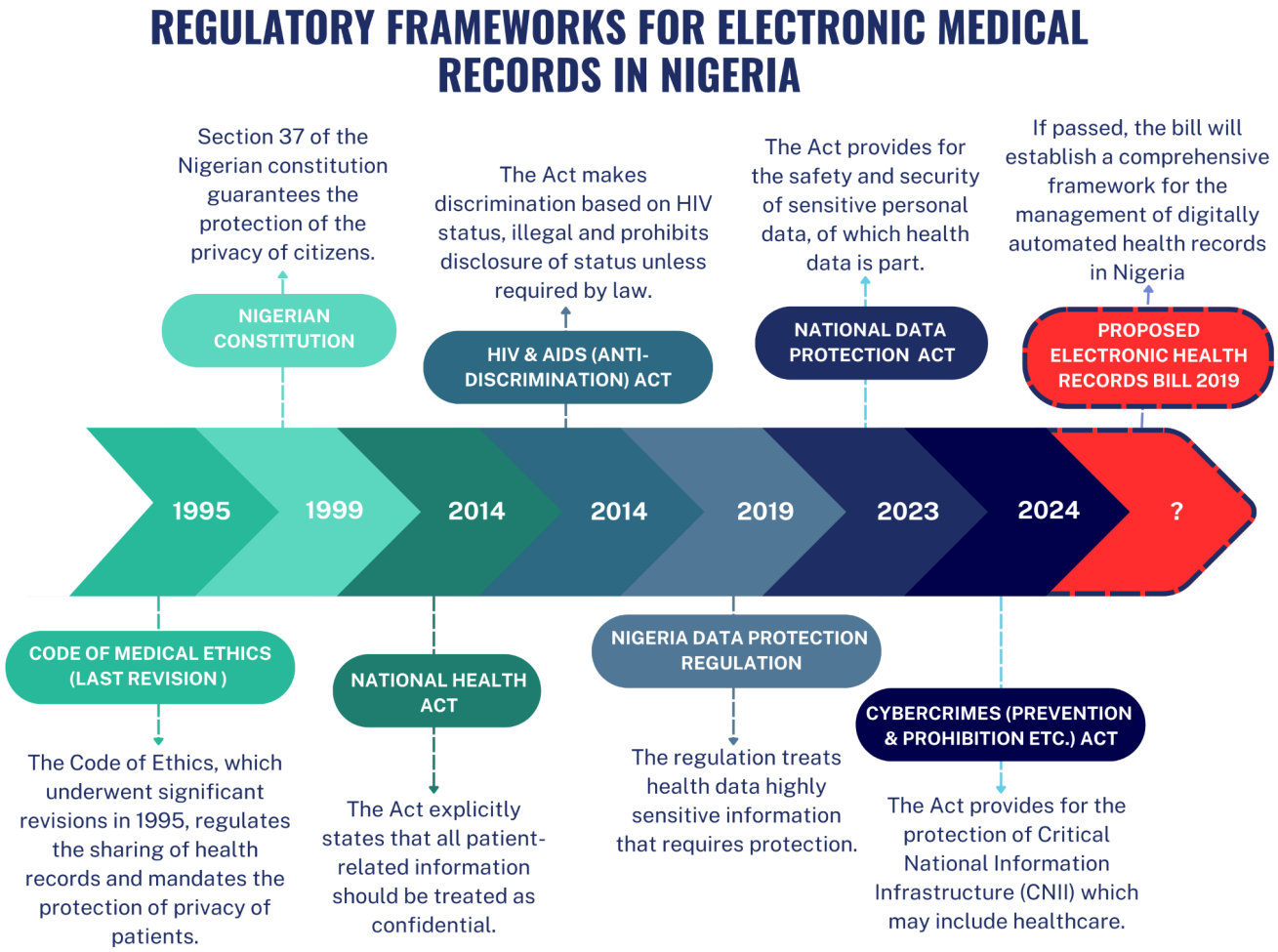
Plateau State Contributory Health Care Management Agency (PLASCHEMA) Data Breach

A significant breach of personal information occurred within Nigeria's healthcare sector involving PLASCHEMA (Plateau State Contributory Health Care Management Agency). The breach exposed the personal data of thousands of citizens, as uncovered by the Website Planet research team. PLASCHEMA oversees Plateau State Universal Health Care, which aims to provide affordable healthcare in the region. Unfortunately, 11 of PLASCHEMA's storage buckets lacked essential security measures such as authentication or encryption. Consequently, over 75,000 files were exposed, totalling around 45GB of data. These files contained Personally Identifiable Information (PII) of program applicants from various cities within Plateau State. Among the compromised data were ID cards containing extensive applicant details, including full names, dates of birth, addresses, and more. Additionally, applicant photos were also exposed. This breach impacted over 37,000 individuals, underscoring the vulnerability of personal data within the healthcare sector.5



[5]Peoples Gazette. Nigerian Agency Data Breach Exposes [75,000] Personal Details of Citizens Online . PG [2022]. *https://gazettengr.com/nigerian-agency-data-breach-exposes-75000-personal-details-of-citizens-online/#:~:text=A%20data%20breach%20affecting%20the,the%20Website%20Planet%20research%20team.*

Existing Regulatory Frameworks for Electronic Medical Records in Nigeria



Several legal frameworks in Nigeria shape the current electronic medical records (EMR) landscape. These frameworks regulate their usage and ensure data security. They also provide guidelines and standards for adopting, implementing, and managing EMR systems across healthcare facilities in the country.

01 1999 Constitution of the Federal Republic of Nigeria (As Amended)

The 1999 Constitution of the Federal Republic of Nigeria (As Amended) is the grundnorm in Nigeria, with the right to privacy enshrined in Section 37. This section guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications.[6]

[6] Chapter C23 Laws of the Federation of Nigeria 2004
http://www.nigeria-law.org/ConstitutionOfTheFederalRepublicOfNigeria.htm

02 National Health Act 2014

The National Health Act provides a legal framework for regulating and developing the Nigerian healthcare sector. It contains provisions related to health information management, including electronic medical records.

Section 26(1) of the Act states that all information regarding a patient, including their health status, treatment, or stay in a healthcare facility, is confidential. This legal provision underscores that confidentiality in healthcare is not solely an ethical principle but a matter of legal significance. Section 26(2) outlines specific circumstances under which health records may be disclosed, including obtaining written consent from the patient, a court order, or when non-disclosure threatens public health. This demonstrates the legal framework to safeguard patient confidentiality and the limited conditions for sharing health information.

In addition, Section 27 of the Act provides that health workers or providers who have access to a user's health records may disclose such personal information to any other person, healthcare provider, or health establishment as is necessary for any legitimate purpose within the ordinary course and scope of their duties where such access or disclosure is in the user's interest.

Section 29 of the National Health Act provides for the protection of health records. It states that proper measures must be put in place to ensure that the management of health establishments possessing a user's health records are set up with control measures to prevent unauthorised access to those records and to the storage facility or system by which records are kept. The Act further prescribes a fine of two hundred and fifty thousand Naira (250,000) or a term of two years imprisonment or both as penalties for anyone who fails to perform this function.

03 The HIV and AIDS (Anti-Discrimination) Act 2014

The HIV/AIDS Anti-Discrimination Act 2014 makes it illegal to discriminate against people based on their HIV status. It also prohibits any employer, individual, or organisation from requiring a person to take an HIV test as a precondition for employment or access to services.[7] Section 11 prohibits the disclosure of status without written consent unless required by law. Section 13 guarantees confidentiality for individuals living with HIV or affected by AIDS, safeguarding their health and medical records. Failure to adhere to these provisions constitutes an offence punishable by a fine of not less than ₦500,000 for an individual or ₦1 million for an institution, or imprisonment for a term not exceeding two years, or both.[8]

[7] UNAIDS Update. Nigeria Passes Law to Stop Discrimination Related to HIV. UNAIDS, February 2015. *https://www.unaids.org/en/resources/presscentre/featurestories/2015/february/20150211_nigeria_law#:~:text=The%20HIV%2FAIDS%20Anti%2DDiscrimination,employment%20or%20access%20to%20services.*

04 Cybercrimes (Prevention and Prohibition etc.) Act 2015

Under the Cybercrime Act, specific sectors are labelled as Critical National Information Infrastructure (CNII). Attacking these sectors is a serious offence, carrying hefty penalties: 10 years imprisonment for general attacks and 15 years for those causing severe harm.[9] No fines are allowed. If an attack leads to death, the offender faces life imprisonment. The healthcare sector is part of this critical infrastructure under Part 7.5 of the 2014 National Cybersecurity Strategy.[10] Section 38(5) of the Act provides that service providers should place adequate safeguards to ensure the privacy and security of such data for law enforcement. The Act also prohibits the unlawful interception of electronic messages, identity theft, and impersonation, significantly if they could compromise health records.

05 Nigeria Data Protection Act 2023

The Nigeria Data Protection Act is the primary legislation on data protection in Nigeria. It protects people's rights to the safety and security of their personal information. The Act addresses a range of issues, with a notable provision pertinent to the Health Sector being the processing of Sensitive Personal Data. According to the Act, data processors can process sensitive data only under specific circumstances. These include obtaining consent from the data subject, fulfilling legal obligations of the data controller or data subject, protecting vital interests when consent is not feasible, conducting non-profit activities with safeguards, engaging in legal proceedings, serving substantial public interest or public health needs while respecting human rights, and managing medical care or community welfare with confidentiality considerations. These conditions are designed to ensure the lawful processing of sensitive personal data, especially in healthcare settings, with measures in place to safeguard the rights and interests of data subjects.[11] Section 25(1) of the Data Protection Act, 2023 similarly provides that data controllers and processors must ensure personal data confidentiality, integrity, and availability using appropriate technical and organisational methods.

[8] HIV and AIDS (Anti-Discrimination) Act, 2014.
https://archive.gazettes.africa/archive/ng/2014/ng-government-gazette-dated-2014-11-28-no-125.pdf

[9] Cybercrimes (Prohibition, Prevention etc) Act, 2015 with Ammendment Act 2024.
https://cert.gov.ng/ngcert/resources/CyberCrime Prohibition_Prevention_etc Act 2024.pdf

[10] National Cybersecurity Strategy, 2014
https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Nigeria_2014_NATIO NAL_CYBESECURITY_STRATEGY.pdf

[11] National Data Protection Act, 2023.
https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf

06 Code of Medical Ethics (Rules of Professional Conduct for Medical & Dental Practitioners)

The Medical and Dental Council of Nigeria periodically reviews and prepares a code of conduct for practitioners in the country, as mandated by the Medical and Dental Practitioners Act. The current edition, titled "Rules of Professional Conduct for Medical and Dental Practitioners in Nigeria," underwent significant revisions in 1995 to align with the Council's experiences in disciplinary matters.12

Section 22 of the Code of Ethics addresses telemedicine, recognising its evolving nature in Nigeria. Specifically, Section 22(a) emphasises electronic processing, requiring practitioners to establish adequate security measures for personal information when stored, transmitted, or received via fax, computer, email, or other electronic channels. It mandates ensuring information security before connecting to a network, preventing unauthorised access or interception. However, practitioners are cautioned that email communication over the Internet may be susceptible to interception.13

Section 42 of the Code regulates the sharing of patient health records among healthcare professionals and mandates the protection of patients' privacy.

Section 44 of the Code deals with confidentiality, stating that medical records are strictly for the continuity of patient care and should not be accessed by anyone outside the profession. Disclosure of patient information is only permissible with the patient's informed consent, preferably in writing, except in cases of statutory disease notification. When faced with requests for information, practitioners must prioritise patient privacy, seek consent whenever possible, anonymise data, and minimise disclosures. The duty of confidentiality extends beyond the practitioner's employment and is relevant even after the patient's death. However, there are exceptions where disclosure is necessary to prevent harm to the patient or others, such as imminent danger or criminal activities.14

[12] Code of Medical Ethics (Rules of Professional Conduct for Medical & Dental Practitioners) P.[1] *https://www.mdcnigeria.org/downloads/code-of-conducts.pdf*

[13] Section [22] Code of Medical Ethics (Rules of Professional Conduct for Medical & Dental Practitioners) P.[30–31] *https://www.mdcnigeria.org/downloads/code-of-conducts.pdf*

[14] Section [22] Code of Medical Ethics (Rules of Professional Conduct for Medical & Dental Practitioners) P.[52–54] *https://www.mdcnigeria.org/downloads/code-of-conducts.pdf*

The Proposed Electronic Health Records Bill Of 2019

The National Electronic Health Record Bill of 2019 aims to establish a comprehensive framework for managing digitally automated health records in Nigeria. It will facilitate the collection and storage of health information in digital formats. The bill's primary goal is to enhance the availability and quality of healthcare information and services across various healthcare providers.

However, the bill may face challenges regarding its alignment with current laws, including the Health Records Officers Act. The Health Records Officers Registration Board contends that the Bill overlaps with the provisions of its enabling legislation, which grants the board authority to oversee the health records management profession.

Furthermore, the bill proposes the establishment of new regulatory and database systems, including the National Electronic Health Record System. This system would comprise the National Electronic Health Record System Operating Board, the National Health Repository Service, and the National Electronic Health Record System Register. It would be responsible for operating and managing health records throughout Nigeria.

Challenges of the absence of the National Health Record system

The absence of a National Health Record system presents several challenges:

Fragmented Health Information

With a decentralised system, health information remains fragmented across various healthcare providers and facilities. This fragmentation can lead to incomplete or inaccurate patient records, hindering continuity of care and medical decision-making.

Limited Access to Comprehensive Patient Data

Healthcare providers may need help accessing a patient's complete medical history, including diagnoses, treatment, and medication, particularly if the patient has received care from multiple sources. This can impede the ability to provide timely and appropriate care.

Duplication of Tests and Procedures

Without a centralised health record, patients may undergo unnecessary duplicate tests and procedures because healthcare providers lack access to previous results. This increases healthcare costs and exposes patients to potential risks associated with unnecessary interventions.

Inefficiencies in Healthcare Delivery

Without a national health record system, administrative burdens increase as healthcare providers spend time and resources manually collecting and sharing patient information. This can result in inefficiencies in healthcare delivery, leading to treatment delays and patient dissatisfaction.

Privacy and Security Risks

In a decentralised environment, disparities in data security measures across different healthcare entities may increase the risk of unauthorised access, data breaches, and privacy violations. Without robust security protocols and oversight, patient confidentiality may be compromised.

Barriers to Population Health Management

The lack of comprehensive health data makes it challenging for public health authorities to effectively monitor and address population health needs. This can hinder efforts to identify trends, allocate resources, and implement targeted interventions to improve health outcomes at the population level.

Recommendations

01 Passage of a Policy by the Federal Ministry of Health

1. The Federal Ministry of Health is urged to issue a comprehensive national health privacy and security directive, complementing the Nigerian Data Protection Act 2023 while drawing inspiration from the United States' Health Insurance Portability and Accountability Act (HIPAA). This rule should establish clear standards for protecting, storing, and transferring health data in electronic or physical formats, encompassing administrative, technical, online, and physical safeguards. Key components include defining the legal basis for processing health-related data processing, considerations for cross-border data transfer, guidance on storage and retention of health data, and procedures for breach reporting and user notification provisions. Additionally, initiating heightened transparency and accountability mechanisms will be essential.

2. Section 2 of the National Health Act (NHA) empowers the Federal Ministry of Health to develop guidelines addressing emerging privacy and security concerns in healthcare technology. Sensitisation efforts targeting healthcare practitioners and the public on privacy and security implications are urgently needed. Furthermore, the National Research Ethics Committee, established under Section 33 of the NHA, should define ethical standards, including privacy and security protocols for research. This should encompass robust de-identification strategies to mitigate re-identification risks.

3. Given the significant risks and costs associated with healthcare data breaches, a proactive approach is imperative. This includes prioritizing application and network security, implementing robust encryption measures, and adhering to best security practices. Heightened vigilance and concerted efforts are essential to ensure the proper handling and protection of sensitive health information, safeguarding the privacy and security of millions of individuals.

4. A multi-faceted approach is recommended to enhance Nigeria's electronic health records (EHRs) infrastructure. The Federal Ministry of Health should prioritize enacting comprehensive privacy and security legislation, drawing inspiration from established frameworks like HIPAA, to develop clear standards for protecting health data. Guidelines addressing emerging privacy and security concerns in healthcare technology should be developed, and sensitization efforts should be conducted. A proactive approach to data security, emphasising application and network security, encryption, and best practices, is crucial. Efforts should focus on establishing interoperability standards for seamless data exchange and capacity-building programs to enhance digital literacy among healthcare practitioners. Public-private partnerships and collaboration are vital to leveraging expertise and resources, fostering innovation, and addressing everyday challenges. Implementing these recommendations will strengthen data security, privacy, and the overall quality of healthcare services in Nigeria.

Conclusion

In conclusion, Nigeria's future of electronic health records (EHRs) holds tremendous potential to revolutionise healthcare delivery and improve patient outcomes. As technology advances, integrating EHR systems into healthcare practices is no longer just a trend but a necessity in realising the goal of Universal Health Care (UHC). EHRs offer a centralised platform for securely storing, accessing, and managing patient data, streamlining processes, enhancing care coordination, and facilitating informed decision-making by healthcare providers.

However, the journey towards a robust and comprehensive EHR infrastructure has challenges. Issues such as interoperability, data security, privacy concerns, and disparities in access to technology pose significant obstacles that must be addressed through concerted efforts from healthcare stakeholders, policymakers, technology developers, and the community at large.

Despite the existing legal frameworks governing health records in Nigeria, there remains a critical gap in specific legislation tailored for electronic health records. Introducing the Electronic Health Record Bill in 2019 was a positive step towards addressing this gap, but its progression into law is still pending.

To realise the full potential of EHR systems in Nigeria, policymakers must prioritise the passage of comprehensive legislation addressing electronic health records. This legislation should establish clear standards for protecting, storing, and transferring health data while addressing breach reporting and user notification requirements. Sensitization efforts targeting healthcare practitioners and the public on privacy and security implications are also crucial.

Furthermore, proactive measures such as prioritising data security, implementing robust encryption measures, and fostering public-private partnerships are essential to safeguarding the privacy and security of healthcare data.

By implementing these recommendations and addressing the challenges outlined, Nigeria can strengthen its electronic health records infrastructure, enhance data security and privacy protections, and ultimately improve the delivery of quality healthcare services to its population. This will contribute to realising Universal Health Care (UHC) goals and improve health outcomes nationwide.