ELECTRONIC HEALTH RECORDS IN NIGERIA: AN EXAMINATION OF THE LEGAL AND REGULATORY FRAMEWORK GOVERNING DATA PRIVACY, SECURITY AND INTEROPERABILITY

OZONNADI OSINACHI SAMUEL

2020/LW/14735

BEING A LONG ESSAY SUBMITTED TO THE FACULTY OF LAW, ALEX EKWUEME FEDERAL UNIVERSITY, NDUFU-ALIKE, IKWO IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF LAW (LL.B) DEGREE.

SEPTEMBER 2025

DECLARATION

I, OZONNADI OSINACHI SAMUEL, a Student of the Faculty of Law, Alex Ekwueme Federal University, Ndufu-Alike, Ikwo, Ebonyi State, do hereby declare on my honour, that this project has not been previously presented, either wholly or in part for the award of any other Degree, Diploma, Certificate or Publication in any University, other Higher Institutions or elsewhere.

Signed……

OZONNADI OSINACHI SAMUEL (2020/LW/14735)

CERTIFICATION

This is to certify that this long essay: **ELECTRONIC HEALTH RECORDS IN NIGERIA: AN EXAMINATION OF THE LEGAL AND REGULATORY FRAMEWORK GOVERNING DATA PRIVACY, SECURITY AND INTEROPERABILITY** is an original research carried out by **OZONNADI OSINACHI SAMUEL.** This research is the result of my own investigation which met the regulation governing the award of Bachelor of Law (LL.B Hons), Alex Ekwueme Federal University Ndufu-Alike Ikwo, Ebonyi State, Nigeria.

DR. KELECHI ONYEBULE ---------- ----------
(Supervisor)

DR. KELECHI ONYEBULE ---------- ----------
(Project Coordinator)

PROF ESENI AZU UDU ---------- ----------
(Dean, Faculty of Law)

External Examiner _____ _____

DEDICATION

This work is dedicated to my family and friends who have supported me through every challenge and triumph. To my beloved father, Ozonnadi Samuel Eze, and my wonderful mother, Ozonnadi Maudlin Ebere, your unwavering love and sacrifices have been the foundation of my success. To my siblings, Ozonnadi Esther Ugonna, Ozonnadi Nnabuike Princewill, Ozonnadi Ozioma Joy, and Ozonnadi Udochukwu Moses, thank you for your constant encouragement and inspiration. To my best friend, Okagbue Chioma Genevieve, and friends from school; Smart Omoghafe, Ifechukwu Raphael, Ogbonna Precious, Emenike Suregrace, Empire Smith, Gideon, Saint 4kt, Teenee, and Jagho—your friendship has made this journey not only bearable but filled with joy and laughter. This dedication is to all of you, whose love and support continue to shape my path.

ACKNOWLEDGENT

I would like to express my deepest gratitude to the people who have been instrumental in making this project a success. First, I sincerely thank my able supervisor, Dr. Kelechi Onyegbule, for his invaluable guidance, constructive feedback, and mentorship throughout this project. Your unwavering support and expertise have been a beacon of light in my academic journey.

To my amiable Dean of the Faculty of Law, Professor Eseni Azu Udu, I extend my heartfelt thanks for your guidance and mentorship during my LL.B journey. Your contributions have greatly shaped my academic growth, and for that, I am truly grateful, and may God bless you immensely.

I am also deeply appreciative of my esteemed lecturers: Barr. Ugota G. Awoke, Barr. P.O. Olebara, Assc. Prof Onyekachi Eni, Dr. N. Amadi, Nnaemeka Nweze, Barr. Uwadiegwu Anoke, Barr. Emeka Chukwudifu, Barr. Charity Chinedu-Uhuo, Barr. Chinelo Ekechi Agwu, and Dr. O.T. Eze. Your dedication, tireless efforts, and the knowledge you imparted have played a significant role in shaping my academic experience. I remain profoundly grateful for the impact each of you has had on my educational journey.

Thank you all for your continued support, encouragement, and belief in me.

TABLE OF CONTENTS

Title Page i

Declaration Page ii

Certification Page iii

Dedication Page iv

Acknowledgements v

Table of Contents vi

List of Abbreviations vii

Abstract viii

CHAPTER ONE: INTRODUCTION

1.1 Background to the Study 1

1.2 Statement of the Problem 4

1.3 Research Questions 7

1.4 Aim and Objectives of the Study 8

1.5 Significance of the Study 9

1.6 Scope and Limitations 10

1.7 Research Methodology 12

1.8 Chapter Analysis 14

CHAPTER TWO: CONCEPTUAL, THEORETICAL FRAMEWORK AND LITERATURE REVIEW

2.1 Conceptual Framework 16

2.1.1 Security 16

2.1.2 Data Privacy 19

2.2 Theoretical Framework 22

2.3 Summary and Gap in Literature 26

CHAPTER THREE: LEGAL AND INSTITUTIONAL FRAMEWORK GOVERNING ELECTRONIC HEALTH RECORDS IN NIGERIA

3.1 Legal Framework 28

3.1.1 Constitution of the Federal Republic of Nigeria 1999 (as amended) 28

3.1.2 National Health Act 2014 29

3.1.3 Medical and Dental Practitioners Act 1990 30

3.1.4 Nigeria Data Protection Regulation 2019 31

3.1.5 Cybercrimes (Prohibition, Prevention, etc.) Act 2015 32

3.1.6 Nigeria Data Protection Act 2023 33

3.1.7 National Information Technology Development Agency Guidelines 2007 34

3.2 Institutional Framework 35

3.2.1 Federal Ministry of Health 35

3.2.2 Medical and Dental Council of Nigeria 36

3.2.3 National Information Technology Development Agency 37

3.2.4 Courts 38

3.2.5 Nigerian Data Protection Commission 39

CHAPTER FOUR: ANALYSIS OF DATA PRIVACY, SECURITY, AND INTEROPERABILITY CHALLENGES

4.1 Challenges and Barriers to Electronic Health Records 40

4.1.1 Lack of Specific Legislation 40

4.1.2 Weak Enforcement and Oversight 41

4.1.3 Poor Infrastructure and Funding 42

4.1.4 Low Awareness and Resistance to Change 43

4.1.5 Cyber-security and Data Privacy Risks 44

4.1.6 Lack of Interoperability Standards 45

4.1.7 Ethical and Cultural Challenges 46

4.2 Comparative Analysis with Global EHR Practices 47

4.2.1 South Africa 47

4.2.2 United Kingdom 49

4.2.3 United States of America 51

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

5.1 Summary of Findings 53

5.2 Recommendations 55

5.3 Conclusion 57

LIST OF ABBREVIATIONS

CFRN – Constitution of the Federal Republic of Nigeria 28

EHR – Electronic Health Records 37

FMOH – Federal Ministry of Health 35

GDPR – General Data Protection Regulation 14

HIPAA – Health Insurance Portability and Accountability Act 14

MDCN – Medical and Dental Council of Nigeria 37

NDPA – Nigeria Data Protection Act 43

NDPR – Nigeria Data Protection Regulation 10

NHA – National Health Act 31

NITDA – National Information Technology Development Agency 37

NDPC – Nigerian Data Protection Commission 43

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

The digital age has significantly transformed the healthcare sector across the globe, with the adoption of Electronic Health Records being one of the most impactful innovations[1]. Electronic Health Records (which will be abbreviated as EHR in this research) are digital systems designed to collect, store, manage, and transfer patient health information in a secure and organized manner[2]. They are widely recognized for their potential to enhance the quality of healthcare services by making patient data more accessible, reducing duplication of tests and procedures, promoting efficiency, and improving communication among healthcare providers. In developed countries, EHRs have become central to the delivery of modern, patient-centered healthcare[3]. In contrast, the implementation of such systems in developing countries like Nigeria is still in its early stages and faces multiple legal, technical, and administrative challenges.

In Nigeria, healthcare delivery has long suffered from fragmentation, inefficiency, and a lack of timely access to accurate medical records[4]. Many healthcare institutions continue to rely on paper-based systems that are prone to errors, loss, and duplication. These traditional record-keeping methods often hinder clinical decision-making, delay treatment, and pose significant challenges to continuity of care[5]. Recognizing these limitations, there is growing interest in the

[1] John Brush, Eileen Handberg, Cathleen Biga, Kim Birtcher, Alfred Bove, Paul Casale, Michael Clark et al., *'2015 ACC Health Policy Statement on Cardiovascular Team-Based Care and the Role of Advanced Practice Providers*', (2015) 65(19) *Journal of the American College of Cardiology 2118.*

[2] Tom, Seymour, Dea Frantsvog, and Tod Graeber, *"Electronic Health Records (EHR)"*, (2012) 3(3) *American Journal of Health Sciences 201.*

[3] Benjamins Janine, Annemien Haveman-Nies, Marian Gunnink, Annemieke Goudkuil, and Emely De Vet, 'How the Use of a Patient-Accessible Health Record Contributes to Patient-Centered Care: Scoping Review', (2021) 23(1) *Journal of Medical Internet Research* e17655.

[4] Ruth Onajite, "*Organizational Bottlenecks, Health Data Management, and Electronic Medical Records Adoption in Nigeria"*, (2024) 7(1) *International Journal of Health Records & Information Management*.

[5] Ibid

digitization of health records as a necessary step towards reforming Nigeria's healthcare sector. As efforts to modernize healthcare services intensify, the adoption of EHRs has emerged as a vital component in the pursuit of improved health outcomes, increased accountability, and enhanced data management.

Nevertheless, the digitization of health records introduces serious legal and regulatory concerns, particularly relating to data privacy, information security, and system interoperability[6]. Health data is classified globally as sensitive personal information, requiring robust legal safeguards to prevent misuse, unauthorized access, and breaches[7]. The risk of data exposure in an environment with inadequate cyber-security infrastructure makes it essential for Nigeria to adopt and enforce comprehensive legal and regulatory frameworks. Additionally, system interoperability, the ability of different EHR platforms to communicate and share information seamlessly is a critical factor in the success of any electronic health system[8]. Without such compatibility, the full potential of EHRs to support coordinated care and improve patient outcomes cannot be realized.

To address these challenges, Nigeria has introduced certain legislative instruments aimed at regulating data protection and patient confidentiality. The Nigeria Data Protection Regulation 2019, issued by the National Information Technology Development Agency, is the foremost regulation guiding data privacy in Nigeria[9]. It classifies health data as sensitive personal data and outlines the principles for lawful processing, consent, storage, and security of such information. In parallel, the National Health Act 2014 provides for patient rights, including the confidentiality of health records and conditions for disclosure[10]. These frameworks, though

[6] Reza Faisal, Jose Prieto, and Stephen Julien *'Electronic Health Records: Origination, Adoption, and Progression'*, (2020) *Public Health Informatics and Information Systems* 188.
[7] ISibor Edwina. *"Regulation of Healthcare Data Security: Legal Obligations in A Digital Age,"* (2024) *SSRN* 4957244.
[8] Ibid
[9] Ali GAGA, Thomas. *"A comparative study of data protection laws & policies: a case study of Nigeria."* (2022).
[10] Ibid

significant, are yet to be fully integrated and enforced within the health sector, especially at the institutional and operational levels.

Despite the existence of these laws, the Nigerian healthcare system continues to face significant barriers in enforcing data protection and ensuring the secure use of electronic health systems[11]. There is limited awareness among healthcare workers and patients regarding data rights, and many healthcare providers lack the technical capacity or institutional readiness to comply with data protection standards. Furthermore, the absence of harmonized regulations for system interoperability means that data sharing across hospitals and clinics is minimal, fragmented, and inconsistent[12]. These challenges reflect broader institutional weaknesses in regulatory oversight, infrastructure, and legal implementation.

It is also important to note that Nigeria's health data environment is influenced by international standards and treaties, such as the General Data Protection Regulation of the European Union, which, though not binding, serves as a reference point for developing data protection regimes in emerging economies[13]. As Nigeria increasingly engages in cross-border digital health initiatives, adherence to international data privacy standards becomes even more relevant.

Against this backdrop, this study seeks to critically examine the legal and regulatory framework governing Electronic Health Records in Nigeria, with specific focus on data privacy, security, and interoperability[14]. The research adopts a doctrinal approach, relying on both primary sources such as legislation, case law, policy documents, and treaties and secondary materials including scholarly texts, journals, and reports. The study aims to identify gaps in the existing legal framework, highlight challenges in enforcement, and propose actionable

[11] Smaranda Olarinde, Elisabeta, Emem Anwana, and Udosen Jacob Idem.. *"E-commerce and e-health in Nigeria: Prospects and Challenges of Effective Legislative Framework for Sustainable Development."* (2024 International Conference on Decision Aid Sciences and Applications (DASA). IEEE, 2024).
[12] Akwaowo, Christie Divine, *"Adoption of electronic medical records in developing countries, A multi-state study of the Nigerian healthcare system."* (2022) 4 Frontiers in Digital Health 1017231.
[13] Akintola, Simisola , and Dorcas A. Akinpelu.. *"The Nigerian Data Protection Regulation 2019 and data protection in biobank research."* (2021) 11(3) International Data Privacy Law 310.
[14] Ibid

recommendations for achieving a more secure, effective, and rights-respecting EHR system in Nigeria. Ultimately, the study contributes to the ongoing discourse on health sector reform by offering insights for policymakers, legal experts, and healthcare professionals on how to build a digital health system that aligns with both national and international legal standards.

1.2 Statement of the Problem

The use of Electronic Health Records is growing in Nigeria as part of efforts to modernize the healthcare system and improve the quality of service delivery[15]. However, while EHRs offer many benefits such as quick access to patient information, better coordination of care, and improved health outcomes, they also raise serious legal concerns relating to data privacy, security, and system interoperability[16]. At present, Nigeria lacks a clear and unified legal framework specifically designed to regulate EHRs. Although the Nigeria Data Protection Regulation 2019 provides general rules for data privacy, it does not fully address the unique challenges posed by digital health records[17]. Similarly, the National Health Act 2014 contains provisions on patient confidentiality but does not provide specific guidance on the management and sharing of electronic health data[18]. This legal gap creates confusion and inconsistency in the way health institutions handle sensitive patient information. One major concern is the protection of personal health data from unauthorized access, cyber-attacks, and misuse[19]. Many healthcare facilities in Nigeria do not have strong digital security systems, and there is limited knowledge among staff on data protection standards[20]. This increases the risk of data breaches and undermines patients' trust in the healthcare system. Furthermore, patients are often not

[15] Oreoluwa Olukorode, Sarah, *"Impact of electronic medical records on healthcare delivery in Nigeria: A review."* (2024) 3(9) PLOS Digital Health e0000420.
[16] Edmond Li. "The impact of electronic health record interoperability on safety and quality of care in high-income countries: systematic review." *Journal of medical Internet research* 24.9 (2022)
[17] Akintola, Simisola, and Dorcas Akinpelu. *"The Nigerian Data Protection Regulation 2019 and data protection in biobank research."* (2021) 11(3) International Data Privacy Law 307.
[18] Danuta Mendelson. *"Legal protections for personal health information in the age of Big Data–a proposal for regulatory framework."* (2017) 3(1) Ethics, Medicine and Public Health 40.
[19] Mohd Javaid. *"Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends."* (2023) 1 Cyber Security and Applications 100016.
[20] Ibid

aware of their rights regarding how their health information is collected, stored, and used. Another pressing issue is the lack of system interoperability[21]. In many parts of the country, hospitals and clinics use different EHR platforms that cannot communicate with one another. As a result, medical records cannot be shared easily between healthcare providers. This can delay treatment, lead to repeated medical tests, and negatively affect patient outcomes. The absence of legal standards for interoperability further complicates the development of a national health information system[22]. In addition, there is weak enforcement of existing data protection laws. Regulatory agencies often lack the technical resources and institutional capacity to monitor compliance, investigate violations, and apply sanctions. This legal and regulatory weakness makes it difficult to ensure that patients' rights are protected in the digital health space. Given the sensitive nature of health data and the rapid growth of digital health platforms in Nigeria, there is an urgent need to examine the adequacy of the existing legal and regulatory framework[23]. Without strong legal protections and enforcement mechanisms, the adoption of EHRs may expose patients to serious risks and may fail to meet the goals of improving healthcare delivery. This study therefore seeks to identify and critically analyze the legal gaps, challenges, and opportunities in the regulation of electronic health records in Nigeria. It will also explore how Nigerian law can be strengthened to better protect health data, ensure secure digital practices, and promote the efficient sharing of information among healthcare providers in line with global best practices.

[21] Olaronke Iroju. *"Interoperability in healthcare: benefits, challenges and resolutions."* (2013) 3(1) International Journal of Innovation and Applied Studies 265.
[22] Fulvio Barbarito, *"Implementing standards for the interoperability among healthcare providers in the public regionalized Healthcare Information System of the Lombardy Region."* (2012) 45(4) Journal of biomedical informatics 737.
[23] Ibid

1.3 Research Questions

1. What are the existing legal and regulatory frameworks governing electronic health records in Nigeria?
2. To what extent do current Nigerian laws and policies protect the privacy and security of electronic health information?
3. What hinders the effective implementation and interoperability of electronic health records in Nigeria?
4. How does the Nigerian Law on Electronic Law stand in comparison with South Africa, United Kingdom, and United States of America

1.4 Aim and Objectives of the Study

1. Identify and examine the existing legal and regulatory frameworks that guide the use of electronic health records in Nigeria.
2. Assess the extent to which current Nigerian laws and policies protect the privacy and security of electronic health information.
3. Explore the legal, institutional, and technical challenges that hinder the full implementation and interoperability of electronic health records in Nigeria.
4. Compare Nigeria's legal framework on electronic health records with that of South Africa, the United Kingdom, and the United States of America.

1.5 Significance of the Study

This study is important for several reasons. First, it contributes to the growing conversation on how technology can improve healthcare delivery in Nigeria. By examining the legal and regulatory framework for electronic health records, the study highlights the strengths and weaknesses in the laws that govern how patient information is stored, protected, and shared.

Second, the study is useful for healthcare policymakers and government agencies, as it provides insights into areas where the current laws and policies need to be improved. Understanding the legal gaps will help in designing stronger regulations to protect patients' data and support a more secure and connected healthcare system.

Third, the study will benefit legal practitioners, researchers, and students by adding to the body of legal knowledge in the areas of health law, information technology law, and data protection law. The comparison with countries like South Africa, the United Kingdom, and the United States will provide lessons that can guide legal reforms in Nigeria. The study is important for healthcare providers and data handlers, as it stresses the need for compliance with legal standards on privacy, security, and interoperability. This will help build public trust in electronic health systems and improve service delivery. The study also promotes public awareness on the rights of patients regarding their health data, and encourages stakeholders to work together to create a system that is both efficient and legally sound.

1.6 Scope and Limitations

This study focuses on the legal and regulatory frameworks governing the use of Electronic Health Records (EHRs) in Nigeria**.** It examines existing laws, regulations, and policies` that address issues related to data privacy, security, and interoperability of health information systems within the country. The research analyzes key legal instruments such as the Nigeria Data Protection Regulation (NDPR**)**, the National Health Act**,** and any relevant health data privacy laws affecting EHR implementation. Additionally, the study looks at the legal implications of data-sharing policies within Nigerian healthcare institutions. The study also explores the role of advocacy and healthcare providers in ensuring patient confidentiality and safeguarding sensitive medical data. The comparison of Nigeria's EHR legal framework with those of South Africa, the United Kingdom, and the United States of America provides insights

into global best practices for electronic health information management, highlighting the strengths and weaknesses of Nigeria's current legal position. Moreover, the study assesses the interoperability of electronic health systems across different healthcare providers and evaluates the challenges in aligning them with international standards for data security and patient privacy.

Limitations

1. Limited Practical Case Studies: Given that the legal framework for EHRs in Nigeria is still developing, there is a lack of extensive case law or legal precedents related to EHR implementation and data protection within Nigerian courts. As a result, the study primarily relies on theoretical analysis and available policy documents rather than real-world legal cases.

2. Dynamic Legal Environment: Laws and regulations regarding EHRs and health data privacy in Nigeria are subject to change. As digital health technologies continue to evolve, new legislation or amendments may be introduced after this study, which might not be fully captured in the analysis. Thus, some findings may be outdated if new laws are passed during or after the research period.

3. Jurisdictional Differences: While the study compares Nigeria's legal framework with those of countries like South Africa, the UK, and the USA, the legal systems in these countries differ significantly. The findings related to data privacy and security may not be directly transferable to Nigerian context, as each jurisdiction has unique legal traditions and policy environments**.**

4. Complexity of Legal Interpretation: Electronic health record laws are often complex and subject to varying interpretations. Legal ambiguities in existing Nigerian laws related to health data privacy**,** security measures, and data-sharing practices may hinder the precise application

of the law. Furthermore, the absence of clear jurisprudence can create challenges in determining how laws will be enforced in the healthcare sector.

5. Focus on Legal Aspects: The primary focus of this study is on the legal frameworks**,** policies**,** and regulations surrounding EHRs in Nigeria. While the research examines the technical and operational challenges of implementing EHRs, it does not delve deeply into the clinical, technological, or financial aspects of the EHR systems themselves. The study is limited to legal and regulatory perspectives and does not fully explore technical aspects such as software interoperability **or** infrastructure limitations in Nigerian hospitals.

1.7 Research Methodology

This research adopts the doctrinal legal research methodology, which is the most suitable method for legal studies that involve the examination of laws, statutes, policies, and legal principles. The doctrinal method is focused on analyzing existing legal texts, such as statutes, regulations, case law, international treaties, and policy documents. This approach helps to understand how the law currently operates and what legal provisions are in place to guide the use of electronic health records in Nigeria. The study involves a critical and systematic analysis of both primary and secondary legal sources. The primary sources used in this study include the Nigerian Constitution, the National Health Act, the Nigeria Data Protection Regulation, the Freedom of Information Act, and other laws that relate to health data protection and information sharing in Nigeria. In addition, relevant international legal instruments, such as the General Data Protection Regulation of the European Union and data privacy frameworks from countries like the United States, United Kingdom, and South Africa, are examined for comparative purposes. The secondary sources include journal articles, textbooks, legal commentaries, conference papers, and online publications by reputable academic institutions, health

organizations, and legal experts. These materials help to provide a broader understanding of the issues of data privacy, security, and interoperability in health record systems.

1.8 Chapter Analysis

Chapter one provides the general introduction to the study. It includes the background to the study, explaining the increasing relevance of electronic health records in modern healthcare systems and the need for legal protection of sensitive patient data in Nigeria. This chapter also presents the statement of the problem, research questions, aim and objectives, as well as the significance, scope and limitations, and methodology of the study. It sets the foundation for the entire research and outlines the direction the study will take.

Chapter Two presents a detailed review of relevant literature. It examines the academic and legal writings on electronic health records, health data privacy, data protection laws, and the challenges of implementing interoperability standards. This chapter also explores theoretical frameworks relating to the protection of personal data in health systems. It assesses the legal meaning of EHRs, the benefits and risks associated with their use, and the importance of having strong legal frameworks to govern their use. The review includes both Nigerian and international perspectives, identifying key themes and gaps in the existing body of knowledge.

Chapter Three focuses on the legal and institutional framework governing EHRs in Nigeria. It critically examines relevant laws such as the National Health Act 2014, Medical and Dental Practitioners Act, 1990, National information Technology Development Agency Guidelines, 2007, General Data protection Regulation, 2016. The chapter also considers professional guidelines from health agencies and medical bodies. It evaluates how these laws protect patient privacy, ensure security of health data, and promote data sharing through interoperable systems.

Chapter Four looks into the challenges and barriers to Electronic Health Records. It also presents a comparative analysis of Nigeria's legal framework with those of South Africa, the United Kingdom, and the United States of America. These countries have been selected for comparison due to their more advanced EHR systems and robust data protection regimes. The aim is to highlight global best practices and lessons that Nigeria can adopt to strengthen its own legal framework. This chapter identifies the similarities and differences in legislative approaches and evaluates how these legal systems address privacy, security, and interoperability of EHRs.

Chapter Five contains the summary, findings, conclusion, and recommendations. It provides a summary of the key issues discussed in the research and highlights the major findings. The chapter offers practical legal and policy recommendations aimed at improving Nigeria's EHR governance. These include proposals for legal reform, institutional strengthening, public awareness, and adoption of international standards. The study concludes by emphasizing the need for Nigeria to adopt a more holistic and proactive legal approach to the regulation of electronic health records in order to ensure both patient safety and health system efficiency.

CHAPTER TWO

CONCEPTUAL, THEORETICAL FRAMEWORK AND LITERATURE REVIEW

2.1 Conceptual Framework

This section explores key concepts essential to understanding the foundational elements of healthcare data management. It begins by addressing the significance of security in protecting sensitive health information. The discussion extends to data privacy, emphasizing the importance of safeguarding personal health data in an increasingly digital world. Lastly, the section delves into electronic health records, examining their role in modern healthcare systems and their implications for patient care, data accessibility, and security. Together, these concepts form the core of healthcare data protection and are critical to ensuring the confidentiality, integrity, and availability of patient information.

2.1.1 Security

The term "security" refers to the legal, technical, and administrative measures put in place to protect sensitive health information stored and shared in digital form[24]. Security is essential because health records contain private and often very personal details about patients' lives, including their medical history, diagnoses, treatments, and sometimes even financial or family information[25]. If this data is not properly protected, it may be exposed to unauthorized access, theft, or misuse, which can harm the patient's dignity, safety, and trust in the healthcare system. From a legal perspective, security means that data controllers such as hospitals, clinics, and health tech providers must take steps to guard electronic health records against breaches,

[24] Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, and National Research Council. *For the record: protecting electronic health information*. National Academies Press, 1997.
[25] Ismail Keshta, and Ammar Odeh. "*Security and privacy of electronic health records: Concerns and challenges."* (2021) 22(2) Egyptian Informatics Journal 180.

whether intentional or accidental[26]. These steps include ensuring that only authorized persons can access patient records, that the systems used to store the records are protected from cyber-attacks, and that the data is not lost, altered, or leaked[27]. In Nigeria, laws like the Nigeria Data Protection Regulation and the Cybercrimes Act, 2015, require organizations handling electronic health records to apply security safeguards[28]. These safeguards include using strong passwords, encrypted systems, secure storage, and regular risk assessments. However, these laws are still developing, and enforcement remains a challenge due to limited infrastructure, low awareness, and lack of digital capacity in many health facilities.

Security in EHRs also includes physical, administrative, and technological safeguards. Physical safeguards refer to securing the environment where data is stored (such as locked server rooms), administrative safeguards involve the policies and procedures guiding access to data, and technological safeguards relate to the use of tools such as firewalls, antivirus software, and encryption[29]. These countries provide useful examples of how security can be integrated into the legal framework to protect health information. For Nigeria, achieving strong security in EHRs means not only having good laws but also putting them into practice through proper training, funding, and supervision[30]. It also means balancing security with other important principles such as privacy, access to care, and system interoperability. The concept of security is a central part of the legal discussion on electronic health records[31]. It connects to the protection of patients' rights, the responsibilities of health institutions, and the role of

[26] Scott Kruse, Clemens. *"Security techniques for the electronic health records."* (2017) 41 Journal of medical systems 5.
[27] Martti Lehto. *"Cyber security in healthcare systems."* (Cyber Security: Critical Infrastructure Protection. Cham: Springer International Publishing, 2022) 183.
[28] Ibid
[29] Ismail Keshta, and Ammar Odeh.. "*Security and privacy of electronic health records: Concerns and challenges."* (2021) 22(2) Egyptian Informatics Journal 182.
[30] Attah, Ambrose Ojadale. *"Implementing an electronic health record in a Nigerian secondary healthcare facility. Prospects and challenges."* (2017).
[31] Harman, Laurinda, Cathy Flite, and Kesa Bond. *"Electronic health records: privacy, confidentiality, and security."* (2012) 14(9) AMA journal of ethics 718.

government in enforcing digital health regulations[32]. Without strong security measures, the goals of digital health transformation in Nigeria cannot be achieved.

2.1.2 Data Privacy

Data privacy refers to the legal and ethical responsibility to ensure that individuals have control over how their personal health information is collected, stored, shared, and used[33]. It is a core aspect of patients' rights, and it plays a central role in the development and regulation of electronic health systems in Nigeria and globally[34]. Health information is among the most sensitive categories of personal data[35]. It includes details such as a person's medical history, diagnosis, treatment plans, test results, and even genetic information. If this kind of information falls into the wrong hands or is used without permission, it can lead to embarrassment, discrimination, stigma, or even harm to the patient's physical or mental well-being. Therefore, protecting data privacy is not only a legal requirement but also a moral and human rights obligation. In Nigeria, data privacy in the healthcare sector is still evolving[36].

The Nigeria Data Protection Regulation 2019, issued by the National Information Technology Development Agency, is one of the key documents addressing the issue. The NDPR sets out rules for how personal data, including health data, should be processed. It requires that data must be collected for a clear purpose, stored securely, used only with the subject's consent, and shared only when necessary and lawful. However, the healthcare sector in Nigeria faces many challenges in fully enforcing data privacy standards[37]. Many health institutions still keep poor

[32] Nadezhda Purtova, Eleni Kosta, and Bert-Jaap Koops. *"Laws and regulations for digital health."* (Requirements Engineering for Digital Health 2015) 50.
[33] Lawrence Gostin. *"Health care information and the protection of personal privacy: ethical and legal considerations."* (1997) 127(8 part 2) Annals of Internal Medicine 685.
[34] Ibid
[35] Lawrence Gostin, and James Hodge "Personal privacy and common goods: a framework for balancing under the national health information privacy rule." (2001) 86 Minn. L. Rev. 1439.
[36]Idoko, Benjamin. *"Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria."* (Magna Scientia Advanced Research and Reviews 2024).
[37] Ibid

records of consent, use unprotected systems to store digital information, and lack staff training in data protection laws. In some cases, patients may not even be aware of their rights regarding how their health data is handled. Globally, data privacy in health records is guided by laws such as the General Data Protection Regulation in the European Union and the Health Insurance Portability and Accountability Act in the United States[38]. These laws provide models for strong privacy protections, requiring healthcare providers to inform patients about data collection, seek consent, ensure confidentiality, and allow individuals to access and correct their own data. Data privacy is about protecting the dignity and autonomy of individuals by ensuring that their personal health data is not accessed, used, or disclosed without their informed and lawful consent. It is a foundation for building trust between patients and healthcare providers, especially in an era where digital health systems are becoming the norm[39].

2.1.3 Electronic Health Records

Electronic Health Records are digital versions of patients' paper-based medical records. They are designed to collect, store, and manage a person's health information in an electronic format that can be easily accessed and shared by authorized healthcare professionals[40]. Unlike traditional paper records, EHRs can be updated in real time and contain comprehensive information about a patient's medical history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory test results[41]. In Nigeria and many parts of the world, the shift from paper records to electronic systems is part of a broader effort to modernize the healthcare sector, improve service delivery, reduce medical errors, and

[38] Era Purike, and Loso Judijanto. *"Comparison of data protection policies in europe and the united states: different legal approaches."* (2025) 3(3) Jurnal Komunikasi 15.
[39] Amrit Pokhrel.*"Harmonizing public health with individual liberties: exploring the interplay of right to health, privacy, and autonomy during recent and future pandemics."* (2025) 18(1) International Journal of Human Rights in Healthcare 110.
[40] Vernon Weeks, Richard. *"Electronic health records: managing the transformation from a paper-based to an electronic system."* (2013) 10(1) Journal of Contemporary Management 140
[41] Ibid

enhance patient outcomes[42]. EHRs help doctors make better clinical decisions by giving them quick access to complete and up-to-date patient information. They also make it easier for different healthcare providers to work together when treating the same patient, especially in cases where referrals or emergency care are required. However, while EHRs offer many benefits, they also raise serious legal and ethical concerns, particularly in areas such as data privacy, security, and interoperability[43]. Because these records are stored electronically, they can become targets for cyber-attacks or unauthorized access if proper safeguards are not in place[44]. This is why laws and policies are needed to regulate how EHRs are created, accessed, stored, and shared in a secure and lawful manner[45].

In Nigeria, the use of electronic health records is still at a developing stage[46]. Although some public and private hospitals have started adopting EHR systems, there is no uniform legal framework guiding their use across the country. This has created a gap in the protection of sensitive patient information and has also slowed down the adoption of interoperable health information systems. The Nigeria Data Protection Regulation 2019 provides general data protection principles, but there is still a need for more specific healthcare-related data protection laws to address the unique nature of EHRs[47]. The Electronic health records represent a key innovation in modern healthcare delivery, but they require strong legal and regulatory support to ensure that patients' rights are protected[48]. Understanding the concept of EHRs is

[42] Ajovi Scott-Emuakpor,. *"The evolution of health care systems in Nigeria: Which way forward in the twenty-first century."* (2010) 51(2) Nigerian Medical Journal.
[43] Ann O'Malley and Peter Cunningham. *"Patient experiences with coordination of care: the benefit of continuity and primary care physician as referral source."* (2009) 24 Journal of general internal medicine 170.
[44] Sharma, Rishabh, *"Cyber Security to Safeguard Cyber Attacks."* (2022) 11(2) International Journal of Information Security and Cybercrime (IJISC) 55.
[45] Ibid
[46] Adedeji, Peter, *"Factors influencing the use of electronic health records among nurses in a teaching hospital in Nigeria."* (2018) 12(2) Journal of health informatics in developing countries 5.
[47] Abrahim Abdo. *A framework for health information sharing and privacy preservation using information hiding and differential privacy*. (Diss. Haramaya University, 2023).
[48] Ibid

essential for assessing Nigeria's readiness to move towards a digital health future that is both secure and efficient.

2.2 Theoretical Framework

2.2.1 Theory of Change

The Theory of Change provides a useful guide to understanding how meaningful improvements can be made in this area of Electronic Health Records in Nigeria[49]. The theory is often used in legal and policy-related studies to describe how certain interventions can lead to desired social, institutional, or policy outcomes[50]. It outlines the steps and conditions necessary for a transformation to take place from a present, less desirable situation to a more beneficial one[51]. At present, Nigeria's legal framework for electronic health records faces a number of serious challenges. These include the lack of strong laws to protect data privacy, weak enforcement of existing regulations, and Poor system coordination across healthcare institutions, and limited awareness among both professionals and the public about digital health rights[52]. This creates a situation where sensitive health data is vulnerable to misuse, and healthcare delivery is often inefficient due to poor information sharing between systems[53].

The Theory of Change in this context suggests that these challenges can be addressed through a sequence of targeted actions[54]. First, legal reforms must be carried out to either revise existing laws or enact new ones that are specifically designed to protect electronic health data and

[49] Ibrahim Shehu. *Acceptance of Electronic Health Records for Improving Quality of Health Service Delivery: A Case Study of Aminu Kano Teaching Hospital Kano State, Nigeria*. (Diss. School of Computing and Information Technology, 2016).
[50] Weiss, Janet. *"Theoretical foundations of policy intervention."* (Public management reform and innovation research, theory, and application 1999) 38.
[51] Ibid
[52] Ibid
[53] Ibid
[54] Mhairi Mackenzie, and Avril Blamey. *"The practice and the theory: lessons from the application of a theories of change approach."* (2005) 11(2) Evaluation 158.

regulate its use. Alongside this, there must be effective policy implementation to ensure that these legal provisions are followed in practice. Furthermore, building the capacity of key stakeholders such as healthcare providers, legal professionals, and regulators is necessary to ensure they understand and apply these rules correctly. Another important part of this change process is public education. When people understand their rights to data privacy and how their health records are handled, they are more likely to trust and use digital health systems[55]. Institutions must also be strengthened to provide adequate monitoring and enforcements. This includes giving regulatory agencies like the National Information Technology Development Agency the power and resources they need to oversee compliance[56]. Through these steps, the expected outcome is a health system that is legally sound, technologically efficient, and respectful of patient rights. Legal protections would be improved, electronic health systems would be more secure and interoperable, and trust in the healthcare system would increase. This progression from the current state to a better future state is what the Theory of Change describes[57].

The Theory of Change gives this law project a logical foundation[58]. It explains how specific legal and policy interventions can lead to improvements in the governance of electronic health records[59]. It also highlights that legal change does not happen by chance, it must be carefully planned and supported by practical action and institutional commitment[60]. The Theory of Change helps to explain how Nigeria can move from its current weak and uncoordinated system of electronic health records to a more secure, efficient, and rights-based digital health

[55] Pekka Ruotsalainen, and Bernd Blobel. *"Health information systems in the digital health ecosystem problems and solutions for ethics, trust and privacy."* (2020) 17(9) International journal of environmental research and public health 3006.
[56] Ibid
[57] Ibiid
[58] Funnell, Sue, and Patricia Rogers. *Purposeful program theory: Effective use of theories of change and logic models*. (John Wiley & Sons, 2011).
[59] Ibid
[60] Ibid

system. At present, EHRs in Nigeria suffer from poor legal protection, low awareness of patient data rights, and a lack of system interoperability across healthcare institutions[61]. Using the Theory of Change, we can see that if strong laws are made and enforced, if institutions are trained and strengthened, and if the public is educated about their rights, then trust in EHRs will increase. This will also lead to better data security, improved patient care, and a more transparent healthcare system. The theory shows that change is not automatic, it requires deliberate legal reform, policy implementation, and stakeholder cooperation[62]. Therefore, the Theory of Change provides a clear pathway to improve how EHRs are managed in Nigeria[63].

The Positivist Law Theory

Positivist theory is a legal and ethical framework grounded in the belief that the validity of a rule or law lies in its formal enactment by a recognized authority, rather than in its moral or societal justification.[64] Prominent scholars such as John Austin and Hart argue that laws are commands issued by a sovereign, and must be obeyed as long as they are properly enacted, regardless of whether they are considered morally right or wrong[65]. John Ladd expressed that legal positivists are quick to point out that the practical effect of identifying law with a part of morals is either to nullify existing law in favour of an ideal law, or to elevate all existing law

[61] Igwama, Geneva Tamunobarafiri. *"Integrating electronic health records systems across borders: Technical challenges and policy solutions."* (2024) 4(7) International Medical Science Research Journal 788.
[62] Brinkerhoff, Derick *"Process perspectives on policy change: highlighting implementation."* (1996) 24(9) World Development 1395.
[63] Adedeji, Taiwo, Hamish Fraser, and Philip Scott. *"Implementing electronic health records in primary care using the theory of change: Nigerian case study."* (2022) 10(8) JMIR medical informatics 8.
[64] Kenneth Einar Himma, Legal Positivism. *Internet Encyclopeadia of Philosophy*. Available on https://iep.utm.edu/legalpos/#:~:text=Legal%20positivism%20is%20a%20philosophy,%2C%20reason%2C%20or%20human%20rights. Last Accessed 25 July 2025.
[65] Afamefuna Igwebudu, Robert, and Ignatius Nnaemeka Onwuatuegwu. *"Separation Thesis of Law and Morality in HLA Hart (An Appraisal of HLA Hart's Concept of Law)."* (2020) 3 East African Scholars Journal of Education, Humanities and Literature 349

to the status of what is moral; in other words, the natural-law theorist, they maintain, has to be either a radical revolutionary or an unregenerate reactionary[66].

The Positivist Law Theory plays a significant role in understanding the legal framework surrounding the use of Electronic Health Records and data protection in Nigeria. This theory emphasizes that law is a system of rules created by legitimate authorities, such as governments or legislatures, and is distinct from moral considerations or societal values[67]. In other words, laws are valid not because they are morally just, but because they have been enacted through proper legal procedures and are enforceable by the relevant authorities.

Positivist Law Theory is particularly relevant because it underscores the importance of existing laws and regulations like the Nigeria Data Protection Regulation and the National Health Act in shaping how patient data, including electronic health records, is managed and protected[68]. From a positivist perspective, the effectiveness of these regulations is determined not by their moral alignment or the ideals they pursue, but by their formal establishment, enforcement, and compliance within the Nigerian legal system. This theory also draws attention to the gaps in enforcement and the challenges posed by limited technical infrastructure within the healthcare sector, as outlined in the study. Positivism suggests that while the legal framework exists, its success hinges on how effectively it is implemented and followed by healthcare providers[69]. The theory directs attention to the need for stronger enforcement mechanisms, as the formal rules themselves are not sufficient unless they are actively upheld.

---

[66] Immanuel Kant, *The Metaphysics of Morals: The Metaphysical Elements of Justice; Translated, with an Inroduction by John Ladd* (Indianapolis: Bobbs-Merrill, 1965) xxix.
[67] Arinze-Umobi Carol, and Maurice Okechukwu Izunwa. *"A Critical Analysis of Legal Positivism and Legislative Nihilism's Role in the Development of Assisted Reproductive Technology."* 2024 9 *AFJCLJ* 78.
[68] Kelechi Onyegbule Goodluck. *"Protecting Patient Confidentiality in Nigeria: Legal, Ethical, and Public Health Perspectives."* (2025) 12(2) Journal of Commercial and Property Law 18
[69] Kenneth Einar Himma, Legal Positivism. *Internet Encyclopeadia of Philosophy*. Available https://iep.utm.edu/legalpos/#:~:text=Legal%20positivism%20is%20a%20philosophy,%2C%20reason%2C%20or%20human%20rights. Last Accessed 28 July 2025.

By using Positivist Law Theory, the research can explore how the existing legal framework comprising both primary sources like legislation and secondary sources like academic materials operates within the Nigerian context. It examines how these laws are applied in practice, their limitations in enforcement, and the challenges faced in ensuring compliance with the regulatory guidelines for electronic health records. Ultimately, the theory provides a lens for understanding the formal structure and application of laws related to healthcare data management and the need for further legal reform to improve security and privacy in Nigeria's healthcare system.

2.3 Summary and Gap in Literature

The implementation of Electronic Health Records (EHRs) in Nigeria has been met with several security challenges. Babatope identified issues such as financial constraints, inadequate ICT resources, and unstable power supply as significant barriers to effective EHR implementation in Nigerian healthcare facilities[70]. Similarly, Bada assessed the information security measures in military hospitals in Lagos State, highlighting concerns regarding data protection in EHR systems[71]. Adaji examined the intersection of open science ideals with data privacy, noting that while open data can enhance research, it poses risks to patient confidentiality if not properly managed[72].

Data privacy remains a critical issue in the adoption of EHRs in Nigeria. Ayoola conducted a comparative study between the United States' HIPAA and Nigeria's NDPR, assessing their

[70] Abisola Esther Babatope, Idowu Peter Adewumi, Damola Olanipekun Ajisafe, Kayode Olayiwola Adepoju, and Adetola Rachael Babatope. *"Assessing the factors militating against the effective implementation of electronic health records (EHR) in Nigeria"* (2024) 14(1) Scientific Reports 31398.
[71] Tanwa Bada, Bamigboye, and Osundina. *"Assessment of Information Security in the Use of Electronic Health Records Management."* (2022) 1(1) Adeleke University Journal of Science 38.
[72] Adaji, Aishatu Eleojo. *"Reconciling the ideals of open science with data privacy in the context of health research in Nigeria: A legal analysis."* (2023) 3 Research Square 1.

effectiveness in safeguarding healthcare data[73]. Adetunji emphasized the importance of secure and interoperable health information systems, advocating for robust privacy measures in EHR implementations[74]. Enabulele (2016) assessed the National Health Act, noting its provisions for patient confidentiality and consent, which are essential for protecting data privacy in healthcare settings[75].

The adoption of EHRs in Nigeria is progressing but faces several challenges. Akwaowo investigated the factors influencing clinicians' adoption of EHRs, finding that perceived usefulness and critical success factors significantly impact their intention to adopt EMRs[76]. Adedeji utilized the Theory of Change to develop a framework for EHR implementation in primary care, highlighting the importance of context-specific strategies for successful adoption[77]. Ayamolowo assessed the utilization of EHRs among nurses in a faith-based teaching hospital, identifying factors that influence their effective use[78].

Gap in Literature

This study identifies a significant gap in the literature regarding the comprehensive legal and regulatory analysis of electronic health records in Nigeria. There is a lack of detailed academic work that combines the evaluation of legal instruments, institutional frameworks, and the

[73] Benjamin Idoko, Jennifer Amaka Alakwe, Ogochukwu Judith Ugwu, Joy Ene Idoko, Fedora Ochanya Idoko, Victoria Bukky Ayoola, Ejembi Victor Ejembi, and Tomilola Adeyinka, *"Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria,' s"*, (2024), 11(02) Magna Scientia Advanced Research and Reviews 151.
[74] Adetunji Ademola, Carlisle George, and Glenford Mapp Ezra, *"Addressing the Interoperability of Electronic Health Records: Proposing the TASSIPS Framework,"* (2024) Preprints 1.
[75] Osahon Enabulele, and Joan Emien Enabulele. *"Nigeria's National Health Act: An assessment of health professionals' knowledge and perception,"* (2016) 57(5) Nigerian Medical Journal 260.
[76] Christie Divine Akwaowo, Humphrey Muki Sabi, Nnette Ekpenyong, Chimaobi M. Isiguzo, Nene Francis Andem, Omosivie Maduka, Emem Dan, Edidiong Umoh, Victory Ekpin, and Faith-Michael Uzoka, *"Adoption of electronic medical records in developing countries—A multi-state study of the Nigerian healthcare system*," (2022) 4 Frontiers in Digital Health 1017231.
[77] Taiwo Adedeji, Hamish Fraser, and Philip Scott. *"Implementing electronic health records in primary care using the theory of change: Nigerian case study."* (2022) 10(8) JMIR medical informatics e33491.
[78] Ayamolowo Love, Omolola Irinoye, and Abayomi Olaniyan, *"Utilization of electronic health records and associated factors among nurses in a faith-based teaching hospital, Ilishan, Nigeria,"* (2023) 6(3) JAMIA open ooad059.

operational realities of data privacy, security, and system interoperability in the Nigerian health sector. Also, little effort has been made to compare Nigeria's legal stance with that of jurisdictions such as the United States, United Kingdom, and South Africa in order to draw lessons and identify areas for improvement.

Therefore, this research aims to fill this gap by providing a thorough doctrinal analysis of the existing Nigerian legal frameworks and institutions governing electronic health records. It also seeks to critically examine the extent of alignment with international standards and to offer recommendations for strengthening the legal and policy environment in Nigeria.

CHAPTER THREE

LEGAL AND INSTITUTIONAL FRAMEWORK FOR ELECTRONIC HEALTH RECORDS IN NIGERIA

3.1 Legal Framework

The legal framework governing the protection of personal data, particularly within the healthcare sector, is crucial for ensuring that individuals' privacy rights are safeguarded. This section will explore the major legislative and regulatory instruments that shape the management of personal data in Nigeria, with a particular focus on healthcare. By examining the Nigeria Data Protection Act 2023, the National Health Act, and other related regulations, this chapter highlights the legal requirements for data privacy, security, and consent, and assesses the implications for healthcare providers, data processors, and patients. The framework established by these laws aims to improve trust in healthcare systems, promote accountability, and ensure that sensitive personal data is handled responsibly in an increasingly digital world.

3.1.1 Nigeria Data Protection Act, 2023

The Nigeria Data Protection Act, 2023 is a major step forward in the country's efforts to regulate how personal data is collected, used, and stored across different sectors, including healthcare[79]. It establishes the Nigeria Data Protection Commission as the main regulatory body responsible for overseeing compliance and enforcement of data protection standards across the country[80]. In the context of electronic health records, the Nigerian Data Protection

[79] Prof. Onyemelukwe Cheluchi, and Dotun Bhadmus. *"Nigeria Data Protection Act 2023: relevant provisions for health care delivery in Nigeria."* Health Ethics and Law Consulting, Lagos (2024).
[80] Ibid

Act is particularly important because it defines health data as a category of sensitive personal data, which requires a higher level of protection[81]. EHRs contain confidential and sensitive information such as medical history, test results, diagnoses, and treatments. Therefore, the principles laid out in the Data Protection Act directly apply to how this information should be handled by healthcare providers, insurance companies, technology platforms, and government agencies[82]. Under the Act, all data controllers and processors, those who collect or manage personal data are required to ensure that data is processed lawfully, fairly, and transparently[83]. Specifically for the healthcare sector, this means that patients must give clear consent before their medical data is collected or shared. The law also sets out rules for data minimization, ensuring only relevant health information is collected and retained only for as long as necessary[84].

In terms of data security, the Act mandates the implementation of appropriate technical and organizational measures to protect personal data from loss, misuse, or unauthorized access. This is especially critical in managing EHRs, where breaches of security can lead not only to personal embarrassment or stigma but also to serious legal and ethical consequences[85]. One of the notable contributions of the 2023 Act is the requirement for organizations that handle sensitive data, including hospitals and healthcare IT providers, to conduct Data Protection Impact Assessments[86]. These assessments help identify potential risks to personal data and guide strategies to minimize such risks an essential tool when designing or upgrading EHR systems. Despite these positive steps, the Act does not provide health-sector-specific guidance

[81] Sebastian Haas *"Aspects of privacy for electronic health records."* (2011) 80(2) International journal of medical informatics 26.
[82] Ibid
[83] S. 9(c)
[84] Lawrence Gostin. *"Health care information and the protection of personal privacy: ethical and legal considerations."* (1997) 127(8 part 2) Annals of Internal Medicine 685.
[85] Ismail Keshta, and Ammar Odeh. *"Security and privacy of electronic health records: Concerns and challenges."* (2021) 22(2) Egyptian Informatics Journal 180.
[86] Randolph, Stetson Jay. *Identifying the Role of Healthcare Leaders in Protecting Sensitive Information Within Their Sector*. (Diss. National University, 2024).

on interoperability, digital identity management, or cross-border sharing of medical records[87]. The Nigeria Data Protection Act, 2023 offers a solid foundation for protecting the privacy and security of electronic health records. However, to support full and safe implementation of EHRs in Nigeria, there is a need for health-specific legislation or supplementary regulations that address the unique challenges of the healthcare sector, particularly in terms of interoperability, emergency data access, and ethical data reuse[88]. This Act represents progress, but further reforms are essential to close the gap between Nigeria and international best practices in digital health governance.

3.1.2 General Data Protection Regulation, 2016

The General Data Protection Regulation, which came into effect in May 2018, is one of the most comprehensive and influential data protection laws in the world[89]. It was adopted by the European Union in 2016 to harmonize data privacy laws across Europe and strengthen the control that individuals have over their personal information[90]. The GDPR applies to all organizations, both inside and outside the EU, that collect or process the personal data of EU citizens[91]. As such, it has become a global benchmark for data protection and privacy legislation. The GDPR is highly relevant because it provides a strong legal framework for managing electronic health records, particularly in terms of data privacy, data security, and interoperability the key focus areas of this research[92]. The GDPR categorizes health-related data as a special category of sensitive personal data that must be given additional protection[93].

[87] Ibid
[88] Ibid
[89] Michelle Goddard. *"The EU General Data Protection Regulation (GDPR): European regulation that has a global impact."* (2017) 59(6) International Journal of Market Research 703.
[90] Ibid
[91] Regulation, General Data Protection. "GDPR. 2016
[92] Semantha, Farida Habib, *"A conceptual framework to ensure privacy in patient record management system."* (2021): 165667.
[93] Johan Hansen. *"Assessment of the EU Member States' rules on health data in the light of GDPR."* (2021).

Article 9 of the Regulation prohibits the processing of personal health data unless specific legal conditions are met, such as explicit consent from the data subject, public interest in the area of public health, or for the provision of health or social care[94]. The GDPR emphasizes several important principles that are critical for the lawful processing of EHRs. These include lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. These principles guide how healthcare providers and technology companies should collect, store, and share medical records[95]. A unique feature of the GDPR is the "right to data portability" (Article 20), which allows individuals to request and receive their data in a structured, commonly used, and machine-readable format and to transmit it to another controller. This supports interoperability in health systems and encourages the use of digital health tools that are secure, efficient, and respectful of patient rights. The GDPR also makes it mandatory for data controllers handling sensitive data to conduct a Data Protection Impact Assessment, particularly when new technologies are used in healthcare systems[96]. This aligns closely with best practices for EHR implementation, where risks such as unauthorized access, cyber-attacks, or data loss must be identified and managed proactively[97].

In comparison to Nigeria's current data protection laws such as the Nigeria Data Protection Act, 2023, the GDPR offers a more detailed and sector-specific approach to health data governance[98]. While the Nigerian Act recognizes health data as sensitive and requires consent, it lacks the clear, detailed guidance found in the GDPR regarding health data processing, cross-

[94] Chico, Victoria. *"The impact of the general data protection regulation on health research."* (2018) 128(1) British medical bulletin 109.
[95] Ibid
[96] Branko Marovic, and Vasa Curcin.. *"Impact of the European general data protection regulation (GDPR) on health data management in a European Union candidate country: a case study of Serbia."* (2020) 8(4) JMIR Medical informatics e14604.
[97] Ibid
[98] Aloamaka, Aloamaka. *"Data protection and privacy challenges in Nigeria: Lessons from other Jurisdictions."* (2023) 3(1) UCC Law Journal 281.

border data transfer, data subject rights, and technical standards for interoperability[99]. As Nigeria seeks to improve its healthcare system through the use of electronic health records, the GDPR serves as a model of best practice. It highlights the need for Nigeria to adopt more robust and detailed legislation that protects patient privacy while enabling secure and efficient health data exchange[100]. The GDPR plays a vital role by offering a comparative framework. It helps to identify the strengths and weaknesses in Nigeria's current data protection regime and suggests ways that Nigeria's legal system can evolve to meet the demands of a modern digital healthcare infrastructure[101].

3.1.2 National Health Act, 2014

The National Health Act, 2014, is a major piece of legislation that governs the provision, regulation, and management of health services in Nigeria[102]. It was enacted to establish a legal framework for achieving universal health coverage, ensuring the rights of health care users, and regulating the roles and responsibilities of health professionals, institutions, and government authorities[103]. As one of the earliest comprehensive health laws in Nigeria, the Act provides the foundation for regulating health information systems, including the management and protection of electronic health records. Under the National Health Act, patient confidentiality and the security Ideals with confidentiality of health information, stating that all information concerning a user's health status, treatment, or stay in a health facility is confidential and may not be disclosed without the user's written consent, a court order, or legal

[99] Adekunle Adewumi. *"'Adequate protection': an analysis of Nigeria's data protection laws within an emerging global data protection framework"*. (Diss. 2022).
[100] Ibid
[101] Ibid
[102] National Health Act, 2014
[103] Taylor, Allyn Lise. *"Making the World Health Organization work: a legal framework for universal access to the conditions for health."* (1992) 18(4) American Journal of Law & Medicine 301.

obligation[104]. This provision is central to the subject of this project, as it lays the groundwork for data privacy and security within Nigeria's health system[105].

Sections 26, 27, and 29 of the National Health Act are particularly relevant to the protection of health data. Section 26 emphasizes patient confidentiality, stipulating that all information regarding a patient's health status, treatment, or stay in a health facility is confidential and cannot be disclosed without the patient's written consent, a court order, or a legal obligation[106]. This provision is fundamental to data privacy and sets the legal foundation for protecting patient information in Nigeria's healthcare system. Section 27 mandates healthcare establishments, both public and private, to maintain proper records of patients[107]. However, the Act does not specify the electronic form of such records or provide detailed guidance on how electronic health data should be collected, stored, or transferred[108]. This gap is critical, especially as Nigeria moves toward digital health technologies and the broader adoption of EHRs. Section 29 reinforces the importance of patient consent for the lawful use of personal health data, further strengthening the framework for data privacy[109]. However, unlike international frameworks such as the General Data Protection Regulation or HIPAA, the NHA does not provide in-depth regulations on the use and management of electronic health data or the establishment of a dedicated regulatory body tasked with overseeing electronic health data compliance[110].

[104] James Hodge, Lawrence Gostin, and Peter Jacobson. *"Legal issues concerning electronic health information: privacy, quality, and liability."* (1999) 282(15) Jama 1466.
[105] Ibid
[106] National Health Act 2014
[107] Ibid
[108]Ambinder, Edward. *"Electronic health records."* (2005) 1(2) Journal of oncology practice 57.
[109] Ibid
[110] Igwama, Geneva Tamunobarafiri. *"Integrating electronic health records systems across borders: Technical challenges and policy solutions."* (2024) 4(7) International Medical Science Research Journal 788.

The National Health Act, 2014, plays a foundational role but also exposes the regulatory limitations currently affecting EHR adoption and effectiveness in Nigeria. While the Act provides broad principles for protecting patient information and promoting health system organization, there is a need for clearer regulatory instruments that focus specifically on the challenges of managing electronic health records in a digital age[111]. The National Health Act, 2014 is an important starting point in Nigeria's legal journey toward the regulation of health information systems[112]. However, its lack of specificity on electronic data management makes it necessary to advocate for more comprehensive legal reforms and digital health policies that will close the current regulatory gaps in data privacy, security, and interoperability of electronic health records.

3.1.3 Medical and Dental Practitioners Act, 1990

The Medical and Dental Practitioners Act, 1990, is a significant legal framework in Nigeria that governs the registration, discipline, and professional conduct of medical and dental practitioners[113]. This Act established the Medical and Dental Council of Nigeria, which is the regulatory authority responsible for ensuring that practitioners maintain professional and ethics in the delivery of healthcare services[114]. Although the Act primarily focuses on licensing, regulation, and discipline within the medical and dental professions, it has important implications for the regulation and management of Electronic Health Records in Nigeria[115]. This is because the handling of patient records, whether in paper or electronic format, is a key aspect of professional medical conduct. Under Section 16 of the Act, the Council has the

[111] Ibid
[112] Ibid
[113] Medical and Dental Practitioners Act, 1990.
[114] Ibid
[115] Gbenro, Victor. *Exploring the impact and roles strategic government leadership plays in adoption and use of eHealth in low resource countries: A case study of the medical and dental council of Nigeria as a professional health regulatory agency*. (Diss. 2018).

authority to prescribe standards of professional conduct[116]. This includes the obligation of doctors and dentists to uphold confidentiality, integrity, and ethical handling of patient information. These principles are crucial when dealing with EHRs, as the shift from paper-based records to digital systems increases the risks associated with data breaches, unauthorized access, and misuse of sensitive medical information. In the context of data privacy and security, which are central themes of this research, the Act underscores the ethical responsibility of medical practitioners to safeguard patient data[117]. However, like the National Health Act, the Medical and Dental Practitioners Act does not expressly address the complexities associated with the digital handling of health data[118]. There are no detailed provisions guiding the use, storage, transmission, or sharing of EHRs. This creates a regulatory vacuum, particularly as Nigeria moves toward digitizing its health system without a robust and specific legal framework to match. Furthermore, the Medical and Dental Council of Nigeria, empowered under this Act, could play a stronger role in setting out regulatory guidelines and best practices for the use of EHRs[119]. Such guidelines would help ensure that practitioners understand their duties in a digital environment, including obtaining informed consent, protecting data security, and ensuring interoperability in ways that uphold patients' rights and meet legal standards. The Act also has an indirect connection to interoperability. As more healthcare providers adopt electronic systems, medical professionals are expected to engage in seamless and secure sharing of patient data when necessary, especially in referral cases or emergencies. The absence of clear statutory directions under this Act regarding such practices can lead to misunderstandings, legal conflicts, or inconsistent practices across hospitals and clinics[120]. It

[116] Medical and Dental Practitioners Act, 1990.
[117] Williamson, Steven, and Victor Prybutok. *"Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare."* (2024) 14(2) Applied Sciences 675.
[118] Medical and Dental Practitioners Act, 1990.
[119] Ibid
[120] Havighurst, Clark . *"Practice guidelines as legal standards governing physician liability."* (1991) 54(2) Law and Contemporary Problems 87.

is evident that while the Medical and Dental Practitioners Act, 1990, forms a foundational part of Nigeria's healthcare legal architecture, it needs to be reviewed and possibly amended to reflect the realities of electronic data management. There is a need to integrate explicit provisions that align with global standards for handling EHRs, as seen in frameworks like the General Data Protection Regulation and the Health Insurance Portability and Accountability Act. This Act provides a framework for ethical medical practice in Nigeria but lacks the specific provisions needed to effectively govern the privacy, security, and interoperability of electronic health records in the modern era. Strengthening this Act with EHR-specific guidelines will contribute greatly to the safe and lawful use of digital health data in Nigeria[121].

3.1.4 National Information Technology Development Agency Guidelines, 2007

The National Information Technology Development Agency Guidelines, 2007 represent one of Nigeria's earliest formal efforts to set standards for the use, management, and protection of information technology systems in the country[122]. These guidelines were developed by NITDA, an agency established under the NITDA Act 2007, with the mandate to regulate and coordinate information technology development in Nigeria. The 2007 NITDA Guidelines provided foundational rules and procedures aimed at promoting good IT governance, especially in government ministries, departments, and agencies[123].

The NITDA Guidelines of 2007 are relevant because they addressed key issues such as data protection, system integrity, network security, and access control, all of which are essential to maintaining data privacy and security in digital health systems[124]. Although the guidelines were

[121] Medical and Dental Practitioners Act of 1990.
[122] Eze, Sunday *"Determinant factors of information communication technology (ICT) adoption by government-owned universities in Nigeria: A qualitative approach."* (2013) 25(4) Journal of Enterprise Information Management 427.
[123] National information Technology Development Agency Guidelines, 2007
[124] Ibid

not originally designed specifically for the health sector, they laid the groundwork for developing more sector-specific regulations in later years. One important aspect of the NITDA Guidelines is the emphasis on security protocols in public sector IT projects. It required agencies to develop policies for user authentication, maintain logs of system access, and ensure data encryption and backup. For electronic health records, these principles are crucial. Patient records must be kept confidential, stored in secure systems, and protected from unauthorized access, tampering, or loss. However, it must be noted that the 2007 Guidelines were limited in their scope and enforcement. They lacked binding force and were more advisory in nature[125]. Also, they did not anticipate the rapid expansion of digital services, including electronic health systems, or the complex privacy challenges that arise when sensitive health data is digitized. These limitations led to the development of more modern frameworks, including the Nigeria Data Protection Regulation 2019, which offers clearer, enforceable standards for data privacy and security. Nevertheless, the 2007 NITDA Guidelines remain historically significant as Nigeria's first formal attempt to shape the national IT regulatory landscape and are still referenced in discussions around digital governance[126].

The NITDA Guidelines of 2007 will be critically examined as a foundational legal instrument. This will explore how the guidelines have influenced the design and regulation of electronic health systems and evaluate whether they still hold relevance today or require significant reform to support interoperable, secure, and privacy-compliant EHR systems in Nigeria. The NITDA Guidelines, 2007 played a key role in introducing principles of accountability, risk management, and data protection in Nigeria's public IT systems. Understanding their strengths

[125] Ibid
[126] Ibid

and weaknesses is essential to improving the current legal and regulatory framework for electronic health records in Nigeria

3.2 Institutional Framework

The institutional framework governing the management of electronic health records (EHRs) in Nigeria plays a critical role in ensuring that healthcare data is handled efficiently, securely, and in compliance with legal standards. This framework includes various government agencies, healthcare institutions, and regulatory bodies responsible for implementing and overseeing policies and regulations related to healthcare data. The Nigeria Data Protection Commission, the National Health Insurance Scheme, and other key health-related organizations are integral to ensuring the security and privacy of health information. This section explores the roles, responsibilities, and interactions of the key institutions involved in the regulation and management of electronic health data in Nigeria. It will examine the functions of these institutions in enforcing the legal requirements as well as their effectiveness in addressing challenges such as data security, interoperability, and access to patient information.

3.2.1 Federal Ministry of Health

The Federal Ministry of Health is the primary government body responsible for formulating and implementing national health policies in Nigeria. Its role is central to the regulation and promotion of health services across the country[127]. The Federal Ministry of Health plays a significant institutional role in shaping the legal and regulatory environment for the adoption and implementation of electronic health records[128]. The Ministry has the constitutional

[127] Obalum, Dike Chijoke, Fatima Alkali, and Sunday Kenechukwu Agwu. *"Analysis of Health Care Policies and Strategies in Nigeria."* (2023) 1(1) Journal of Medical Standards and Ethics 20.
[128] Sherer, Susan A., Chad D. Meyerhoefer, and Lizhong Peng. "*Applying institutional theory to the adoption of electronic health records in the US."* (2016) 53(5) Information & Management 570.

responsibility to provide leadership in the health sector by developing strategic plans, health policy frameworks, and operational guidelines for healthcare delivery[129].

In recent years, the Federal Ministry of Health has embraced the potential of digital health tools to improve health service delivery, particularly in areas like patient record management, disease surveillance, and service coordination. Through various initiatives, such as the Health Information System Policy and the National Health ICT Strategic Framework, the Ministry sets standards for the digitization of health records and supports efforts to transition from paper-based systems to electronic platforms. In relation to data privacy and security, the Ministry collaborates with other regulatory bodies like the National Information Technology Development Agency and the Nigeria Data Protection Bureau to ensure that health data collected through digital systems are handled responsibly[130]. The Ministry recognizes that patient health information is sensitive and must be protected from unauthorized access, misuse, or loss. Therefore, it plays an advocacy and supervisory role in ensuring compliance with relevant laws and regulations guiding data protection within healthcare institutions[131].

The Federal Ministry of Health supports interoperability by encouraging health facilities especially public hospitals to adopt unified digital health platforms. Interoperability refers to the ability of different health information systems to work together and exchange patient data securely and accurately[132]. The Ministry's role in facilitating data harmonization and standard setting is crucial to achieving this goal. However, despite its responsibilities and initiatives, the Ministry faces challenges such as inadequate funding, poor infrastructure, lack of skilled personnel, and limited awareness among healthcare workers about data privacy laws. These

[129] Ibid
[130] Ibid
[131] Ibid
[132] Barbarito, Fulvio. *"Implementing standards for the interoperability among healthcare providers in the public regionalized Healthcare Information System of the Lombardy Region."* (2012) 45(4) Journal of biomedical informatics 736.

issues affect the effective rollout and governance of electronic health records in Nigeria. The Federal Ministry of Health serves as a key institution in the development and supervision of EHRs in Nigeria[133]. It is responsible not only for setting policies that encourage digital health adoption but also for ensuring that health data is managed in a secure, private, and interoperable manner. Its efforts, in coordination with other agencies, are essential to strengthening the legal framework for health data governance in Nigeria[134].

3.2.2 Medical and Dental Council of Nigeria

The Medical and Dental Council of Nigeria is a statutory regulatory body established by the Medical and Dental Practitioners Act, Cap M8, Laws of the Federation of Nigeria 2004[135]. The Council is primarily responsible for regulating the practice of medicine, dentistry, and alternative medicine in Nigeria. It plays a vital role in setting and maintaining the standards of professional practice and ethics for medical and dental practitioners[136]. The role of MDCN becomes relevant when examining how electronic health records intersect with professional ethics, patient confidentiality, data security, and record-keeping responsibilities. One of the core duties of MDCN is to ensure that practitioners adhere to strict ethical guidelines when handling patient information[137]. As medical records are increasingly digitized through the use of EHRs, the Council's regulatory function must extend to ensuring that healthcare professionals are trained in the ethical and secure use of digital technologies in managing patient data. The MDCN, therefore, has a duty to update its codes of conduct and professional

[133] Ojadale Attah, Ambrose. *"Implementing an electronic health record in a Nigerian secondary healthcare facility. Prospects and challenges."* (2017): 5.
[134] Ibid
[135] Medical and Dental Council of Nigeria, 2004.
[136] Friday Ojonugwa, Agbo, Dr Gwom, and Solomon Gwom.*"The role and challenges of the National Agency for Food and Drug Administration and regulation of alternative medicine in Nigeria." World Health* (2021): 25.
[137] Shubayli, Miral Yahya Ahmed, Fatmah Ibrahim Mousa Kamili, and Bayan Hamad Ail Aashwa. *"roles and responsibilities of medical records staff in healthcare settings."* (2024) 6(2) Tec Empresarial 664.

standards to reflect modern technological practices, including how patient health information is recorded, stored, shared, and protected.

In relation to data privacy and security, the Council's guidelines reinforce the importance of confidentiality, a fundamental aspect of the doctor-patient relationship[138]. With the advent of EHRs, confidentiality now involves not just verbal or written information, but also electronically stored and transmitted data. Thus, medical and dental professionals are expected to follow laid-down rules regarding access control, patient consent, and disclosure procedures in line with existing privacy regulations, such as the Nigeria Data Protection Act and the National Information Technology Development Agency Guidelines. The MDCN also collaborates with other government bodies, such as the Federal Ministry of Health and NITDA, to create awareness and training programs for practitioners on the importance of data protection, cyber-security, and the ethical implications of digital health practices. This coordination is essential in promoting interoperability the safe and seamless exchange of health information among authorized healthcare providers while still safeguarding patient rights[139].

Furthermore, the Council needs to play a stronger role in monitoring compliance and ensuring that both public and private medical institutions integrate EHR systems that are aligned with national data governance standards. The Medical and Dental Council of Nigeria plays an important institutional role in guiding how electronic health records are handled within the Nigerian healthcare system. Its influence lies in professional regulation, ethical oversight, and its contribution to national discussions on data privacy, security, and interoperability. To fully

[138] Ibid
[139] Ibid

realize the benefits of EHRs while protecting patient rights, the MDCN must continue to evolve in response to digital health advancements[140].

3.2.3 Data Protection Officers

In the modern digital age, where personal information is often collected, stored, and shared electronically, the role of Data Protection Officers has become very important especially in sectors like healthcare where sensitive personal data is handled daily[141]. Within the Nigerian legal framework, the establishment of DPOs is guided primarily by the Nigeria Data Protection Act and the National Information Technology Development Agency Guidelines 2007, which seek to ensure that organizations manage personal data responsibly and lawfully[142]. A Data Protection Officer is an individual appointed within an organization to oversee compliance with data protection laws.

In the context of electronic health records, DPOs play a key role in ensuring that hospitals, clinics, and healthcare-related agencies comply with the legal and ethical rules concerning the privacy, security, and proper handling of patient data. Their responsibilities include advising the organization on its data protection obligations, monitoring internal data processing activities, and serving as a contact point between the organization and regulatory authorities like NITDA. In Nigeria's healthcare system, the DPO helps to make sure that the use of EHRs follows the required data protection principles, such as lawful processing, data minimization, accuracy, storage limitation, and integrity and confidentiality. For example, if a hospital wants to share a patient's record with another health facility, the DPO must ensure that the patient's

[140] Ibid
[141] Radi Romansky. *"Digital age and personal data protection."* (2022) 14(3) International Journal on Information Technologies & Security 89.
[142] National Information Technology Development Agency Guidelines 2007,

consent has been obtained, and that the data will be transmitted through secure channels to prevent unauthorized access[143].

Furthermore, DPOs are expected to conduct data protection impact assessments before any new digital health systems are introduced, especially those that involve large-scale processing of sensitive health information. This ensures that potential risks to patient privacy are identified and addressed early. DPOs also help organizations respond to data breaches, including notifying affected individuals and reporting to the appropriate authorities within the time allowed by law. However, despite the clear importance of DPOs, many Nigerian healthcare institutions still lack proper awareness or full implementation of this role[144]. There are challenges such as insufficient training, lack of enforcement mechanisms, and limited resources in some healthcare facilities[145]. Strengthening the legal mandate and capacity of DPOs is therefore essential for improving trust in Nigeria's digital health infrastructure. Data Protection Officers serve as a critical part of Nigeria's data governance system, especially in the healthcare sector where electronic health records are increasingly adopted. Their role supports compliance, accountability, and the protection of patient rights, aligning closely with the goals of this research in examining how legal and regulatory frameworks can safeguard digital health information in Nigeria.

3.2.3 Courts

The court is a fundamental institution in any legal system, including Nigeria's. It serves as the primary dispute resolution body and plays a vital role in the interpretation and enforcement of laws[146]. In the context of Electronic health records, the court is an important institution for

[143] Ibid
[144] Ibid
[145] Ibid
[146] Olufunke Adeola Kehinde, and Modupe Nancy Wiwoloku. *"Alternative Dispute Resolution: Historical and Contemporary Perspectives on Enhancing the Role of Traditional Rulers in Nigeria." Štát a právo*: 200.

ensuring that the legal and regulatory frameworks governing data privacy, data security, and interoperability are properly upheld[147]. Courts in Nigeria are empowered by the Constitution and other statutes to handle cases related to breaches of data protection, violations of privacy rights, and medical negligence involving electronic data[148]. When a person's electronic health record is accessed without their permission, or when their sensitive health information is leaked due to poor data handling, the affected individual may seek legal redress through the courts[149].

The Nigerian judicial system consists of several levels of courts, including the Magistrate Courts, High Courts, Court of Appeal, and the Supreme Court. For cases involving data privacy and electronic health, the Federal High Court usually has jurisdiction, especially when the case concerns violations of federal laws such as the Nigeria Data Protection Act or matters relating to information and communication technology[150]. The courts also play a critical role in the interpretation of laws, particularly where there are gaps, ambiguities, or conflicts within Nigeria's data protection and health information regulations[151]. Through judicial decisions, the courts can provide clarity on how legal provisions should be applied in real-life cases. This is important in a fast-changing area like digital health, where new technologies often raise complex legal and ethical issues. Moreover, the court provides a platform where individuals, civil society organizations, and regulatory bodies like the National Information Technology Development Agency can seek judicial review of policies or actions by healthcare providers, technology companies, or even government institutions that may not comply with data

[147] Ibid
[148] Nwankwo, Iheanyi Samuel. *"Information privacy in Nigeria."* (African Data Privacy Laws 2016): 50.
[149] Hodge James, Lawrence Gostin, and Peter Jacobson *"Legal issues concerning electronic health information: privacy, quality, and liability."* (1999) 282(15) Jama 1466.
[150] Ibid
[151] Adekunle Adewumi. *"'Adequate protection': an analysis of Nigeria's data protection laws within an emerging global data protection framework."* (Diss. 2022).

protection laws. In this way, the court acts as a check and balance mechanism in the protection of digital health rights[152].

However, it is important to note that accessing justice through the courts in Nigeria sometimes faces challenges such as delay in court processes, limited judicial capacity in data protection law, and lack of technical expertise among legal practitioners and judges on digital health systems[153]. These limitations can affect the effectiveness of the court in resolving electronic health data issues promptly and fairly. The court is a key institution for enforcing the legal rights of individuals in relation to their electronic health records[154]. It provides an avenue for accountability, justice, and the protection of privacy and security under the law. As Nigeria continues to embrace digital health technologies, the role of the court will become even more significant in upholding trust in the legal system and ensuring that the rights of patients are respected and protected.

[152] Ibid
[153] Olalekan Bello, and Cecile Ogufere. *"The Emerging Artificial Intelligence Legal-Judicial System's Interface: Assessing the State of Nigeria's Judicial System's Readiness for a Revolution."* (2024):6.
[154] William Roach. *Medical records and the law*. (Jones & Bartlett Publishers, 2006).

CHAPTER FOUR

ANALYSIS OF DATA PRIVACY, SECURITY, AND INTEROPERABILITY CHALLENGES

4.1 Challenges and barriers to Electronic Health Records

The adoption and effective use of Electronic Health Records (EHRs) in Nigeria face several challenges that limit their full potential in improving healthcare delivery, protecting patients' rights, and ensuring data security[155]. Although the idea of digitizing health information promises better efficiency, accuracy, and continuity of care, many obstacles legal, technical, financial, and institutional continue to slow down progress[156].

4.1.1. Lack of Specific Legislation

One major challenge is the absence of a comprehensive law specifically focused on electronic health records[157]. While there are general laws on data protection, such as the Nigeria Data Protection Act 2023, these do not address the unique issues related to health data[158]. Unlike countries like the United States and the United Kingdom, Nigeria does not have legislation that outlines how EHRs should be created, stored, shared, or secured within the health sector[159]. This legal gap creates uncertainty for healthcare providers and patients, and increases the risk of rights violations.

[155] Ajayi Sima, and Tayyebe Tadi. "Barriers for adopting electronic health records (EHRs) by physicians." (2013) 21(2) *Acta Informatica Medica* 129.
[156] Velthoven Van, Michelle Helena, Carlos Cordon, and Goutam Challagalla.. "Digitization of healthcare organizations: The digital health landscape and information theory." (2019) 124 *International journal of medical informatics* 49.
[157] Ben Assuli Ofir. "Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments." (2015) 119(3): *Health policy* 287.
[158] Ibid
[159] Ibid

4.1.2. Weak Enforcement and Oversight

Even where relevant guidelines and regulations exist, enforcement is often weak. Institutions like the National Information Technology Development Agency (NITDA) and the Federal Ministry of Health have roles to play in overseeing compliance, but lack the technical and financial capacity to monitor all healthcare providers[160]. There are few penalties for non-compliance, and most hospitals and clinics are not regularly audited for how they manage patient data[161]. This weak oversight creates opportunities for data misuse, negligence, or breaches of confidentiality[162].

4.1.3. Poor Infrastructure and Funding

Many healthcare facilities in Nigeria, especially those in rural areas, lack the infrastructure to support electronic recordkeeping[163]. Challenges such as unreliable electricity, poor internet connectivity, and outdated computer systems make it difficult to run digital health systems effectively[164]. Moreover, the high cost of purchasing and maintaining EHR software discourages investment by private and public hospitals. Without adequate funding, the implementation of EHRs will continue to be limited to only a few urban centers[165].

[160] Neeta Barporika, "Role of Information Technology in Enhancing Healthcare Services." *Digital Technologies for a Resource Efficient Economy* (USA: IGI Global, 2024), 63.
[161] Benjamin Idoko, Jennifer Amaka Alakwe, Ogochukwu Judith Ugwu, Joy Ene Idoko, Fedora Ochanya Idoko, Victoria Bukky Ayoola, Ejembi Victor Ejembi, and Tomilola Adeyinka, "Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria." (2024) *Magna Scientia Advanced Research and Reviews* 8.
[162] James Hodge Jr., Lawrence Gostin, and Peter Jacobson, "Legal issues concerning electronic health information: privacy, quality, and liability." (1999) 282(15) *Jama* 1466.
[163] Ambrose Ojadale Attah. Implementing an electronic health record in a Nigerian secondary healthcare facility. Prospects and challenges (Norway: UiT The Arctic University of Norway, 2017):12.
[164] Ibid
[165] Ibid

4.1.4. Low Awareness and Resistance to Change

There is still low awareness among healthcare workers and patients about the benefits and risks of electronic health records[166]. Many health professionals are more comfortable with manual recordkeeping and may resist switching to digital systems due to fear of technology, lack of training, or concerns about job security[167]. Patients, too, may not trust digital systems to protect their private health information, especially when they hear about cyber- attacks or data breaches in the news[168].

4.1.5. Cyber-security and Data Privacy Risks

Electronic records are vulnerable to cyber-attack, hacking, and unauthorized access[169]. In Nigeria, there have been several cases of data leaks and breaches across different sectors, and the health sector is not immune[170]. Without strong cyber-security policies, encryption methods, and technical standards, patients' sensitive health information may be at risk. This can lead to serious consequences such as identity theft, blackmail, or discrimination[171].

---

[166] Entzeridou Eleni, Evgenia Markopoulou, and Vasiliki Mollaki."Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security." (2018) 110 *International journal of medical informatics* 100.
[167] Ibid
[168] Raul Luha, Emily Rhine, Matthew Myhra, Ross Sullivan, and Clemens Scott Kruse, "Cyber threats to health information systems: A systematic review." (2016) 24(1) *Technology and Health Care* 5.
[169] Mustafa Mhara, Abdullah Abdulrahman, and Abdulhakim Baroud."Cyber Attacks and Threats: Study Of The Types Of Cyber Attacks: Hacking, Viruses, Targeted Attacks, And Electronic Espionage." (2024) *Int. J. Electr. Eng. and Sustain* 40.
[170] Tosin Clement, Callistus Obunadike, Darlington C. Ekweli, Oluomachi E. Ejiofor, Oluwadamilola Ogunleye, Simo Sevidzem Yufenyuy, and C. J. Obunadike. "Cyber Analytics: Modelling the Factors behind Healthcare Data Breaches for Smarter Security Solutions." (2024) 10(1) *International Journal of Advance Research, Ideas and Innovations in Technology* 50.
[171] Nifakos Sokratis, Krishna Chandramouli, Charoula Konstantina Nikolaou, Panagiotis Papachristou, Sabine Koch, Emmanouil Panaousis, and Stefano Bonacina "Influence of human factors on cyber security within healthcare organisations: A systematic review." (2021) 21(15) *Sensors* 5119.

4.1.6. Lack of Interoperability Standards

Another major barrier is the lack of standard formats and procedures that allow different health systems to communicate with each other[172]. In many cases, hospitals use different software that cannot share patient data with one another[173]. This creates delays and fragmentation in patient care, especially when a patient is referred from one facility to another[174]. A lack of interoperability also limits the government's ability to collect health data for national planning and research[175].

4.1.7. Ethical and Cultural Challenges

In some communities, cultural beliefs about illness and confidentiality can affect how people view electronic records[176]. Some patients may be unwilling to allow their data to be stored electronically due to mistrust or fear of stigmatization. Additionally, ethical questions arise regarding who owns patient data, how long it should be stored, and who can access it[177].

[172] Clement McDonald. "The barriers to electronic medical record systems and how to overcome them." (1997) 4(3) *Journal of the American Medical Informatics Association* 215.
[173] Ibid
[174] Ibid
[175] Rajesh Sharma, and Prabin Kumar Panigrahi. "Developing a roadmap for planning and implementation of interoperability capability in e-government." (2015) 9(4) *Transforming Government: People, Process and Policy* 430.
[176] Laurinda Harman, Cathy A. Flite, and Kesa Bond, "Electronic health records: privacy, confidentiality, and security." (2012) 14(9) *AMA journal of ethics* 712.
[177] Ibid

4.2 Comparative Analysis with Global EHR Practices

4.2.1 South Africa

In understanding how Nigeria can improve the legal and institutional framework guiding Electronic Health Records (EHRs), it is important to examine how other countries with similar social and economic structures are managing their EHR systems. South Africa is a suitable case study because it is a fellow African country that has made notable progress in digitizing health information. By comparing Nigeria's approach to that of South Africa, this analysis aims to point the lapses, best practices, and possible lessons that Nigeria can adopt in the development of its own EHR legal framework.

South Africa's Legal Framework for EHRs

South Africa has established a more defined legal and policy framework for electronic health data[178]. One of the most important laws in South Africa is the Protection of Personal Information Act 2013[179]. This Act provides specific rules on how personal data, including health records, should be collected, stored, processed, and shared[180]. POPIA recognizes health information as sensitive personal data and imposes strict obligations on healthcare providers to ensure data security, confidentiality, and lawful processing[181]. Additionally, South Africa's National Health Act 2003 provides a legal basis for maintaining health records and empowers the Department of Health to create national health information systems[182]. Under this Act, health facilities are

[178] Katurura, Munyaradzi C., and Liezel Cilliers. "Electronic health record system in the public health care sector of South Africa: A systematic literature review." (2018) 10(1): *African journal of primary health care & family medicine* 5.
[179] Ciara Staunton, Rachel Adams, Dominique Anderson, Talishiea Croxton, Dorcas Kamuya, Marianne Munene, and Carmen Swanepoel. "Protection of Personal Information Act 2013 and data protection for health research in South Africa." (2020) 10(2) *International Data Privacy Law* 165.
[180] Protection of personal information Act, 2013.
[181] Nokuthula Olorunju. "Data security: the protection of personal health information in the healthcare system." (2019) 54(3) *Journal of Public Administration* 363.
[182] National Health Act, 2003.

required to protect the confidentiality of patient records and may only disclose such information under specific legal conditions, such as with patient consent or a court order[183].

Institutional Framework

South Africa's Department of Health plays an active role in the development and implementation of health information systems[184]. The country has developed a Health Normative Standards Framework (HNSF)**,** which sets the technical standards for data exchange and interoperability across health systems. This helps ensure that data from one hospital or clinic can be shared with +another in a safe and standardized way, improving patient care and coordination. In addition to government efforts, South Africa has partnered with international organizations such as the World Health Organization (WHO) and donor agencies to build infrastructure for digital health. These collaborations have helped improve funding, training, and awareness around EHRs[185].

Implementation and Practical Experience

Unlike Nigeria, where EHR adoption is still largely limited to private hospitals in urban areas, South Africa has made more progress in implementing EHR systems in public healthcare facilities. Some provinces in South Africa have rolled out pilot programs for electronic health records that are connected to a central health database. While the process is not without challenges, including budget constraints and staff resistance, South Africa's progress shows that political commitment, legal clarity, and institutional support can improve EHR outcomes even in resource-limited settings.

[183] Ibid
[184] Graham Wright, Don O'Mahony, and Liezel Cilliers "Electronic health information systems for public health care in South Africa: a review of current operational systems." (2017) 4(1) *Journal of Health Informatics in Africa* 10.
[185] Ibid

4.2.2 United Kingdom

To better understand the gaps in Nigeria's legal and institutional framework for electronic health records (EHRs), it is useful to compare with countries that have more advanced systems. The United Kingdom (UK) is a good case study because it has one of the most developed and structured EHR systems in the world. By studying how the UK has managed the legal, technical, and institutional aspects of EHRs, Nigeria can learn important lessons that may help improve its own health data systems.

Legal Framework in the UK

In the UK, the protection of electronic health records is mainly guided by the Data Protection Act 2018, which is the UK's version of the General Data Protection Regulation[186]. This law treats health information as special personal data, meaning it is more sensitive and needs higher protection. The law requires healthcare providers to collect and use patient data only for legal, fair, and specific purposes[187]. It also gives patients the right to know what information is being stored, how it is used, and the right to correct or delete wrong information[188].

The National Health Service also has specific data protection rules and guidelines for all hospitals and clinics. For example, before a patient's data can be shared, consent must be obtained, unless the law requires otherwise. There are also strong rules on who can access patient records, and systems must be designed to ensure data is safe from cyber threats[189].

[186] Chris Jay Hoofnagle, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius. "The European Union general data protection regulation: what it is and what it means." (2019) 28(1) *Information & Communications Technology Law* 28.1 65.
[187] Ibid
[188] Ibid
[189] Rodrigues, Joel, Isabel De La Torre, Gonzalo Fernández, and Miguel López-Coronado. "Analysis of the security and privacy requirements of cloud-based electronic health records systems." (2013) 15 (8) *Journal of medical Internet research* 186.

Institutional Framework

The NHS Digital, now called NHS England, is the main body responsible for managing and protecting electronic health records in the UK[190]. It works with hospitals, private care providers, and other public agencies to ensure data is stored, transferred, and used safely[191]. The UK government also created the role of the Data Protection Officer (DPO), which every public health body must have[192]. The DPO ensures that the organization follows all data protection laws and reports any breach[193]. There are also bodies like the Information Commissioner's Office (ICO), which is an independent regulator. The ICO monitors how well the NHS and other bodies are complying with data protection laws[194]. If any institution fails to protect health data properly, the ICO can investigate and issue penalties[195].

Implementation and Digital Health Practices

The UK has a long history of using digital technology in healthcare. The NHS launched one of its first EHR programs in the 2000s[196]. Although some of the early projects had challenges, recent developments have shown great improvement. Many NHS hospitals now use shared care records, where patient information is available across different health facilities[197]. This improves patient safety, reduces duplication, and speeds up care delivery[198].For example, a patient who

[190] David Wyatt, David, Scott Lampon, and Christopher McKevitt, "Delivering healthcare's 'triple aim': Electronic health records and the health research participant in the UK National Health Service." *Sociology of health & illness* 42.6 (2020): 1312.
[191] Ibid
[192] Korff Douwe, and Marie Georges, *The Data Protection Officer* (Italy; European Union, 2019): 5.
[193] Ibid
[194] David Erdos "Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government's Statutory Reform Plans," (2022) 16 *University of Cambridge Faculty of Law Research Paper* 32
[195] Ibid
[196] Scott Evans, "Electronic health records: then, now, and in the future," (2016) 25 *Yearbook of medical informatics* S48.
[197] Leigh Warren, Jonathan Clarke, Sonal Arora, and Ara Darzi, "Improving data sharing between acute hospitals in England: an overview of health record system distribution and retrospective observational analysis of inter-hospital transitions of care." (2019) 9(12): *BMJ open* e031637.
[198] Ibid

visits a new clinic in a different city can have their medical history retrieved instantly from a central database, provided proper consent is given. In addition, patients in the UK have access to NHS apps, which allow them to view their medical history, prescriptions, and test results from their phones[199].

4.2.3 United States of America

To improve the legal and institutional framework guiding Electronic Health Records (EHRs) in Nigeria, it is useful to study how other countries have approached similar challenges. The United States of America (USA) provides a relevant case because it has made significant progress in the digitization of health records and the protection of health data through legislation and technology. By examining how the USA has managed its EHR system, Nigeria can learn useful lessons to strengthen its own legal and regulatory frameworks.

Legal Framework in the United States

In the USA, the protection of electronic health records is mainly governed by a law known as the Health Insurance Portability and Accountability Act (HIPAA**)**, passed in 1996[200]. HIPAA provides strong rules to protect patients' health information[201]. It ensures that health data is kept private and secure and that it is only shared when necessary and legal. The HIPAA law has special rules for electronic records, requiring health facilities and service providers to install security systems to prevent unauthorized access to patient data[202]. Another law, called the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, was

[199] Ibid
[200] Jacquelyn O'herrin, Norman Fost, and Kenneth Kudsk, "Health Insurance Portability Accountability Act (HIPAA) regulations: effect on medical record research." (2004) 239 (6) *Annals of surgery* 772.
[201] Ibid
[202] Health Insurance Portability and Accountability Act, 1996.

introduced to promote the adoption of EHRs across the country[203]. It provides financial support and legal guidance to healthcare providers to help them transition from paper records to digital systems. HITECH also increased the penalties for failing to protect electronic health information, showing the importance the USA places on data privacy and security[204].

Institutional Framework

In the United States, there are several government agencies responsible for overseeing EHRs. The Office for Civil Rights (OCR) under the U.S. Department of Health and Human Services (HHS) enforces HIPAA rules and investigates complaints related to the misuse of health information[205]. The HHS also oversees health IT programs and provides standards for how electronic records should be created, stored, and shared. Additionally, the Office of the National Coordinator for Health plays vital role in setting the technical standards and promoting interoperability[206]. Interoperability means that different hospital systems can share patient data safely and easily when needed. This office ensures that electronic health systems across the country work together efficiently and securely[207].

[203] Londsey Hoggle, *The Health Information Technology for Economic and Clinical Health (HITECH) Act* (USA: Congressional Research Service, Library of Congress, 2009), 1935.
[204] Janine Hiller, Matthew McMullen, Wade Chumney, and David Baumer, "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared." (2011) 17 *BUJ Sci. & Tech. L.* 1.
[205] Justin Pope, "Top Five HIPAA Lessons Learned: A Review of HHS Resolution Agreements," (2020) 17(7-9) *Innovations in clinical neuroscience* 45.
[206] Ibid
[207] Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, and National Research Council. *For the record: protecting electronic health information*. National Academies Press, 1997.

Technology and Practice in the USA

In practice, the USA has achieved a high level of digital health adoption. Most hospitals and clinics use EHR systems to manage patient records. These systems are connected through national networks, allowing authorized doctors to access a patient's medical history in real time. This reduces the risk of medical errors and makes treatment faster and more accurate. Patients also have access to their own health records through secure online portals[208]. They can view their test results, schedule appointments, and communicate with healthcare providers through mobile apps and websites. This level of transparency and access helps build trust between patients and healthcare providers[209].

[208] Ibid
[209] Ibid

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Summary of Findings

This research has examined the legal and regulatory framework surrounding the use of Electronic Health Records (EHRs) in Nigeria, with a focus on data privacy, security, and system interoperability. After an in-depth doctrinal analysis of statutes, policies, guidelines, and relevant institutional roles, both domestic and international, several findings have emerged. First, the study found that Nigeria lacks a comprehensive and unified legal framework specifically designed to govern Electronic Health Records. While there are general data protection laws such as the Nigeria Data Protection Regulation (NDPR) 2019, and older guidelines like the NITDA Guidelines of 2007, these do not fully address the unique legal challenges posed by electronic health systems, especially with respect to interoperability, enforcement, and cross-border data sharing. Second, the Federal Ministry of Health, the Medical and Dental Council of Nigeria (MDCN), and other relevant bodies have made some efforts to regulate aspects of health record-keeping. However, these institutions still operate in silos, with limited coordination or unified standards on how patient health data should be collected, stored, secured, and accessed in digital form. Furthermore, it was discovered that Data Protection Officers (DPOs), who are required to monitor compliance with data protection rules, are not yet fully integrated into healthcare institutions across Nigeria. This gap weakens internal oversight and accountability in the handling of sensitive health information. Moreover, the institutional role of the courts was found to be underutilized in resolving data privacy and health information disputes. There is a limited number of judicial decisions or precedents that clarify how existing laws apply to EHRs, resulting in legal uncertainty for both patients and health institutions.

From a global perspective, this study's comparative analysis revealed that countries such as the United States, United Kingdom, and South Africa have implemented more structured and enforceable EHR regulations. These countries have achieved greater success through detailed legislation, dedicated regulatory agencies, and financial investments in health IT infrastructure. In contrast, Nigeria's health sector still faces challenges such as inadequate infrastructure, poor funding, limited awareness among healthcare professionals, and the absence of national standards for interoperability. Finally, the research identified significant security risks and privacy concerns in the Nigerian healthcare sector due to weak enforcement of existing data protection laws, low digital literacy among health workers, and poor cyber-security measures in public and private hospitals.

5.2 Recommendations

1. Nigeria should enact a comprehensive law dedicated to Electronic Health Records (EHRs) that addresses privacy, security, consent, and interoperability.
2. Regulatory bodies like the Federal Ministry of Health and NITDA must be strengthened with technical and financial resources to enforce compliance.
3. All healthcare facilities should be mandated to appoint Data Protection Officers (DPOs) to ensure accountability in managing patient data.
4. National interoperability standards should be developed to enable seamless data sharing across hospitals and clinics.
5. Government should invest in digital infrastructure, including reliable electricity and internet, particularly in rural health facilities.
6. Regular audits and penalties for non-compliance must be implemented to improve enforcement and deter data misuse.

7. Training and continuous professional development programs should be introduced to build digital literacy among healthcare workers.
8. Public awareness campaigns should be launched to educate patients on the benefits and protections of electronic health records.
9. Nigeria should promote public–private partnerships to fund EHR systems, software development, and capacity-building initiatives.
10. Strong cybersecurity policies, including encryption and secure authentication, must be enforced to protect sensitive health data from breaches.

5.3 Conclusion

This research set out to examine the legal and regulatory framework that governs Electronic Health Records (EHRs) in Nigeria, focusing on issues of data privacy, information security, and interoperability. In doing so, the study adopted a doctrinal methodology, reviewing statutes, policy documents, judicial decisions, and institutional practices. It also drew comparisons from more developed EHR systems in South Africa, the United Kingdom, and the United States. The findings show that Nigeria is still at an early stage in the development and regulation of electronic health records. Although some legal instruments, such as the Nigeria Data Protection Regulation (NDPR), and policy guidelines from agencies like NITDA exist, they are not specifically tailored to meet the complexities of digital health data management. Furthermore, there is a lack of coordination among health-related institutions such as the Federal Ministry of Health and the Medical and Dental Council of Nigeria regarding the regulation and supervision of electronic health systems. It has become clear that there is no single, comprehensive legal framework in Nigeria that regulates EHRs holistically. Issues of consent, patient access, third-party data sharing, cyber-security, and interoperability are either inadequately addressed or completely absent in the current legal structure. Moreover,

enforcement remains weak, and many healthcare providers have not adopted or implemented digital record-keeping systems due to infrastructure and resource constraints. The comparative analysis revealed that while countries like the United Kingdom and the United States have made significant progress in securing health data and promoting EHR interoperability, Nigeria has much to learn and implement. These countries have developed specific legislation, regulatory agencies, and funding structures that support EHR adoption and protection. In conclusion, while Nigeria has taken initial steps toward protecting electronic health data, much more is required to build a strong, enforceable, and adaptable legal framework. Such a framework should reflect international best practices and be supported by adequate institutional oversight, public awareness, and technical infrastructure. Without urgent legal reform and capacity-building, the full benefits of EHRs such as improved healthcare delivery, data-driven decision-making, and patient safety may not be realized in Nigeria.

BOOKS

Abrahim Abdo. *A framework for health information sharing and privacy preservation using information hiding and differential privacy*. (Diss. Haramaya University, 2023).

AdekuAdetunji Ademola, Carlisle George, and Glenford Mapp Ezra, *"Addressing the Interoperability of Electronic Health Records: Proposing the TASSIPS Framework,"* (Preprints 2024).

Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, and National Research Council. *For the Record: Protecting Electronic Health Information*. (National Academies Press 1997).

ISibor Edwina. *"Regulation of Healthcare Data Security: Legal Obligations in A Digital Age,"* (*SSRN* 2024) 4957244.

Korff Douwe, and Marie Georges, *The Data Protection Officer* (Italy; European Union, 2019): 5.

Londsey Hoggle. *The Health Information Technology for Economic and Clinical Health (HITECH) Act*. (USA: Congressional Research Service, Library of Congress. 2009)

Martti Lehto. Cyber security in healthcare systems. In *Cyber Security: Critical Infrastructure Protection* (Cham: Springer International Publishing. 2022) 183

Nadezhda Purtova, Eleni Kosta, and Bert-Jaap Koops. *"Laws and regulations for digital health."* (Requirements Engineering for Digital Health 2015) 50.

Neeta Barporika, "Role of Information Technology in Enhancing Healthcare Services." *Digital Technologies for a Resource Efficient Economy* (USA: IGI Global, 2024), 63.

Nwankwo, Iheanyi Samuel. *"Information privacy in Nigeria."* (African Data Privacy Laws 2016): 50.

Olufunke Adeola Kehinde, and Modupe Nancy Wiwoloku. *"Alternative Dispute Resolution: Historical and Contemporary Perspectives on Enhancing the Role of Traditional Rulers in Nigeria." Štát a právo*: 200.

Smaranda Olarinde, Elisabeta, Emem Anwana, and Udosen Jacob Idem.. *"E-commerce and e-health in Nigeria: Prospects and Challenges of Effective Legislative Framework for Sustainable Development."* (2024 International Conference on Decision Aid Sciences and Applications (DASA). IEEE, 2024).

Weiss, Janet. *"Theoretical foundations of policy intervention."* (Public management reform and innovation research, theory, and application 1999) 38.

William Roach. *Medical records and the law*. (Jones & Bartlett Publishers, 2006).

JOURNALS

Abisola Esther Babatope, Idowu Peter Adewumi, Damola Olanipekun Ajisafe, Kayode Olayiwola Adepoju, and Adetola Rachael Babatope. "Assessing the factors militating against the effective implementation of electronic health records (EHR) in Nigeria*" Scientific Reports* 14, no. 1 (2024) 31398.

Adaji, Aishatu Eleojo. "Reconciling the ideals of open science with data privacy in the context of health research in Nigeria: A legal analysis." *Research Square* 3, (2023) 1

Adedeji, Peter. "Factors influencing the use of electronic health records among nurses in a teaching hospital in Nigeria." *Journal of Health Informatics in Developing Countries*, 12, no. 2 (2018) 5.

Adedeji, Taiwo, Hamish Fraser, and Philip Scott. "Implementing electronic health records in primary care using the theory of change: Nigerian case study." *JMIR Medical Informatics* 10, no. 8 (2022) 8.

Afamefuna Igwebudu, Robert, and Ignatius Nnaemeka Onwuatuegwu. "Separation Thesis of Law and Morality in HLA Hart (An Appraisal of HLA Hart's Concept of Law." *East African Scholars Journal of Education, Humanities and Literature* 3, (2020) 349

Ajayi, Sima, and Tayyebe Tadi. "Barriers for adopting electronic health records (EHRs) by physicians." *Acta Informatica Medica*, 21, no. 2 (2013) 129.

Ajovi, Scott-Emuakpor. "The evolution of health care systems in Nigeria: Which way forward in the twenty-first century?" *Nigerian Medical Journal*, 51, no. 2 (2010).

Akintola, Simisola, and Dorcas A. Akinpelu. "The Nigerian Data Protection Regulation 2019 and data protection in biobank research." *International Data Privacy Law*, 11, no. 3 (2021) 307/310.

Akwaowo, Christie Divine. "Adoption of electronic medical records in developing countries: A multi-state study of the Nigerian healthcare system." *Frontiers in Digital Health*, 4, (2022) 1017231.

Aloamaka, Aloamaka. "Data protection and privacy challenges in Nigeria: Lessons from other jurisdictions." *UCC Law Journal*, 3, no. 1 (2023) 281.

Ambinder, Edward. "Electronic health records." *Journal of Oncology Practice*, 1, no. 2 (2005) 57.

Amrit Pokhrel. "Harmonizing public health with individual liberties: Exploring the interplay of right to health, privacy, and autonomy during recent and future pandemics." *International Journal of Human Rights in Healthcare*, 18, no. 1 (2025) 110.

Ann O'Malley and Peter Cunningham. "Patient experiences with coordination of care: The benefit of continuity and primary care physician as referral source." *Journal of General Internal Medicine*, 24, (2009) 170.

Arinze-Umobi, Carol, and Maurice Okechukwu Izunwa. "A critical analysis of legal positivism and legislative nihilism's role in the development of assisted reproductive technology." *AFJCLJ*, 9, (2024) 78.

Ayamolowo Love, Omolola Irinoye, and Abayomi Olaniyan. “Utilization of electronic health records and associated factors among nurses in a faith-based teaching hospital, Ilishan, Nigeria.” *JAMIA Open*, 6, no. 3 (2023) ooad059.

Barbarito, Fulvio. “Implementing standards for the interoperability among healthcare providers in the public regionalized healthcare information system of the Lombardy Region.” *Journal of Biomedical Informatics*, 45, no. 4 (2012), 736.

Ben Assuli, Ofir. “Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments.” *Health Policy*, 119, no. 3 (2015) 287.

Benjamin Idoko, Jennifer Amaka Alakwe, Ogochukwu Judith Ugwu, Joy Ene Idoko, Fedora Ochanya Idoko, Victoria Bukky Ayoola, Ejembi Victor Ejembi, and Tomilola Adeyinka. “Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria.” *Magna Scientia Advanced Research and Reviews*, 11, no. 02/8 (2024) 151.

Benjamins, Janine, Annemien Haveman-Nies, Marian Gunnink, Annemieke Goudkuil, and Emely De Vet. “How the use of a patient-accessible health record contributes to patient-centered care: Scoping review.” *Journal of Medical Internet Research*, 23, no. 1 (2021) e17655.

Branko Marovic, and Vasa Curcin. “Impact of the European General Data Protection Regulation (GDPR) on health data management in a European Union candidate country: A case study of Serbia.” *JMIR Medical Informatics*, 8, no. 4 (2020) e14604.

Brinkerhoff, Derick. “Process perspectives on policy change: Highlighting implementation.” *World Development*, 24, no. 9 (1996) 1395.

Chico, Victoria. “The impact of the General Data Protection Regulation on health research.” *British Medical Bulletin*, 128, no. 1 (2018) 109.

Chris Jay Hoofnagle, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius. “The European Union General Data Protection Regulation: What it is and what it means.” *Information & Communications Technology Law*, 28, no. 1 (2019) 65.

Christie Divine Akwaowo, Humphrey Muki Sabi, Nnette Ekpenyong, Chimaobi M. Isiguzo, Nene Francis Andem, Omosivie Maduka, Emem Dan, Edidiong Umoh, Victory Ekpin, and Faith-Michael Uzoka, “Adoption of electronic medical records in developing countries—A multi-state study of the Nigerian healthcare system,” *Frontiers in Digital Health* 4 (2022) 1017231.

Ciara Staunton, Rachel Adams, Dominique Anderson, Talishiea Croxton, Dorcas Kamuya, Marianne Munene, and Carmen Swanepoel. “Protection of Personal Information Act 2013 and data protection for health research in South Africa”. *International Data Privacy Law*, 10, no. 2 (2020) 165.

Clement McDonald. “The barriers to electronic medical record systems and how to overcome them.” *Journal of the American Medical Informatics Association*, 4, no. 3 (1997) 215.

Danuta Mendelson. “Legal protections for personal health information in the age of Big Data: A proposal for regulatory framework.” *Ethics, Medicine and Public Health*, 3, no. 1 (2017) 40.

David Erdos. (2022). “Towards effective supervisory oversight? Analyzing UK regulatory enforcement of data protection and electronic privacy rights and the government’s statutory reform plans.” *University of Cambridge Faculty of Law Research Paper*, 16, (2022) 32

David Wyatt, David, Scott Lampon, and Christopher McKevitt. “Delivering healthcare’s ‘triple aim’: Electronic health records and the health research participant in the UK National Health Service.” *Sociology of Health & Illness*, 42, no. 6 (2020) 1312.

Edmond Li. “The impact of electronic health record interoperability on safety and quality of care in high-income countries: Systematic review.” *Journal of Medical Internet Research*, 24, no. 9 (2022).

Entzeridou Eleni, Evgenia Markopoulou, and Vasiliki Mollaki. “Public and physician’s expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security.” *International Journal of Medical Informatics*, 110 (2018) 100.

Era Purike, and Loso Judijanto. “Comparison of data protection policies in Europe and the United States: Different legal approaches.” *Jurnal Komunikasi*, 3, no.3 (2025) 15.

Eze, Sunday. “Determinant factors of information communication technology (ICT) adoption by government-owned universities in Nigeria: A qualitative approach.” *Journal of Enterprise Information Management*”, 25, no. 4 (2013) 427.

Fulvio Barbarito. (2012). “Implementing standards for the interoperability among healthcare providers in the public regionalized healthcare information system of the Lombardy Region.” *Journal of Biomedical Informatics*, 45, no. 4 (2012) 737.

Graham Wright, Don O'Mahony, and Liezel Cilliers. “Electronic health information systems for public health care in South Africa: A review of current operational systems.” *Journal of Health Informatics in Africa*, 4, no. 1 (2017) 10.

Harman, Laurinda, Cathy Flite, and Kesa Bond. “Electronic health records: Privacy, confidentiality, and security.” *AMA Journal of Ethics*, 14, no. 9 (2012) 718.

Havighurst, Clark. “Practice guidelines as legal standards governing physician liability.” *Law and Contemporary Problems*, 54, no. 2 (1991) 87.

Hodge, James, Lawrence Gostin, and Peter Jacobson. “Legal issues concerning electronic health information: Privacy, quality, and liability.” *JAMA* 282, no. 15 (1999) 1466.

Igwama, Geneva Tamunobarafiri. “Integrating electronic health records systems across borders: Technical challenges and policy solutions.” *International Medical Science Research Journal*, 4, no. 7 (2024) 788.

Ismail Keshta, and Ammar Odeh. “Security and privacy of electronic health records: Concerns and challenges.” *Egyptian Informatics Journal*, 22, no. 2 (2021) 180/182.

Jacquelyn O’Herrin, Norman Fost, and Kenneth Kudsk. (1999). “Health Insurance Portability Accountability Act (HIPAA) regulations: Effect on medical records.” *JAMA*, 282, no. 15 (1999) 1466.

James Hodge, Lawrence Gostin, and Peter Jacobson. "Legal issues concerning electronic health information: privacy, quality, and liability." *Jama* 282, no. 15 (1999) 1466.

Janine Hiller, Matthew McMullen, Wade Chumney, and David Baumer. “Privacy and security in the implementation of health information technology (electronic health records): US and EU compared.” *BUJ SCI. & Tech L.*, 17, (2011) 1.

John Brush et al. “2015 ACC Health Policy Statement on Cardiovascular Team-Based Care and the Role of Advanced Practice Providers.” *Journal of the American College of Cardiology*, 65, no. 19 (2015) 2118.

Justin Pope. “Top Five HIPAA Lessons Learned: A Review of HHS Resolution Agreements.” *Innovations in Clinical Neuroscience*, 17, no. 7-9 (2020) 45.

Katurura, Munyaradzi C., and Liezel Cilliers. “Electronic health record system in the public health care sector of South Africa: A systematic literature review.” *African Journal of Primary Health Care & Family Medicine*, 10, no. 1 (2018), 5.

Kelechi Onyegbule Goodluck. “Protecting patient confidentiality in Nigeria: Legal, ethical, and public health perspectives.” *Journal of Commercial and Property Law*, 12, no. 2 (2025) 18.

Laurinda Harman, Cathy A. Flite, and Kesa Bond. “Electronic health records: Privacy, confidentiality, and security.” *AMA Journal of Ethics*, 14, no. 9 (2012) 712.

Lawrence Gostin, and James Hodge. “Personal privacy and common goods: A framework for balancing under the national health information privacy rule.” *Minnesota Law Review*, 86 (2001) 1439.

Lawrence Gostin. “Health care information and the protection of personal privacy: Ethical and legal considerations.” *Annals of Internal Medicine*, 127, no. 8 part 2 (1997) 685.

Leigh Warren, Jonathan Clarke, Sonal Arora, and Ara Darzi. “Improving data sharing between acute hospitals in England: An overview of health record system distribution and retrospective observational analysis of inter-hospital transitions of care.” *BMJ Open*, 9, no. 12, e031637.

Mhairi Mackenzie, and Avril Blamey. “The practice and the theory: Lessons from the application of a theories of change approach.” *Evaluation*, 11, no 2 (2005) 158.

Michelle Goddard. “The EU General Data Protection Regulation (GDPR): European regulation that has a global impact.” *International Journal of Market Research*, 59, no. 6 (2017) 703.

Mohd Javaid. “Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends.” *Cyber Security and Applications*, 1 (2023) 100016.

Mustafa Mhara, Abdullah Abdulrahman, and Abdulhakim Baroud. “Cyber attacks and threats: Study of the types of cyber attacks: Hacking, viruses, targeted attacks, and electronic espionage.” *International Journal of Electrical Engineering and Sustain*, (2024) 40.

Nifakos Sokratis, Krishna Chandramouli, Charoula Konstantina Nikolaou, Panagiotis Papachristou, Sabine Koch, Emmanouil Panaousis, and Stefano Bonacina. “Influence of human factors on cyber security within healthcare organisations: A systematic review.” *Sensors*, 21, no. 15 (2021) 5119.

Nokuthula Olorunju. “Data security: The protection of personal health information in the healthcare system.” *Journal of Public Administration*, 54, no. 3 (2019) 363.

Obalum, Dike Chijoke, Fatima Alkali, and Sunday Kenechukwu Agwu. “Analysis of health care policies and strategies in Nigeria.” *Journal of Medical Standards and Ethics*, 1, no. 1 (2023) 20.

Olaronke Iroju. “Interoperability in healthcare: Benefits, challenges, and resolutions.” *International Journal of Innovation and Applied Studies*, 3, no.1 (2013) 265.

Oreoluwa Olukorode, Sarah. “Impact of electronic medical records on healthcare delivery in Nigeria: A review.” *PLOS Digital Health*, 3, no. 9 (2024) e0000420.

Osahon Enabulele, and Joan Emien Enabulele. “Nigeria's National Health Act: An assessment of health professionals' knowledge and perception.” *Nigerian Medical Journal*, 57, no. 5 (2016) 260.

Pekka Ruotsalainen, and Bernd Blobel. “Health information systems in the digital health ecosystem: Problems and solutions for ethics, trust, and privacy.” *International Journal of Environmental Research and Public Health*, 17, no. 9 (2020) 3006.

Radi Romansky. “Digital age and personal data protection.” *International Journal on Information Technologies & Security*, 14, no. 3 (2022) 89.

Rajesh Sharma, and Prabin Kumar Panigrahi. “Developing a roadmap for planning and implementation of interoperability capability in e-government.” *Transforming Government: People, Process and Policy*, 9, no. 4 (2015) 430.

Raul Luha, Emily Rhine, Matthew Myhra, Ross Sullivan, and Clemens Scott Kruse. “Cyber threats to health information systems: A systematic review.” *Technology and Health Care*, 24, no. 1 (2016) 5.

Rodrigues, Joel, Isabel De La Torre, Gonzalo Fernández, and Miguel López-Coronado. “Analysis of the security and privacy requirements of cloud-based electronic health records systems.” *Journal of Medical Internet Research*, 15, no. 8 (2013) 186.

Ruth Onajite. *Organizational bottlenecks, health data management, and electronic medical records adoption in Nigeria. International Journal of Health Records & Information Management*, 7, no. 1 (2024).

Scott Evans. “Electronic health records: Then, now, and in the future.” *Yearbook of Medical Informatics*, 25 (2016) S48.

Scott Kruse, Clemens. “Security techniques for the electronic health records.” *Journal of Medical Systems*, 41, no. 1 (2017) 5.

Sebastian Haas. “Aspects of privacy for electronic health records.” *International Journal of Medical Informatics*, 80, no. 2 (2011) 26.

Sharma, Rishabh. “Cyber security to safeguard cyber attacks.” *International Journal of Information Security and Cybercrime (IJISC)*, 11, no. 2 (2022) 55.

Sherer, Susan A., Chad D. Meyerhoefer, and Lizhong Peng. “Applying institutional theory to the adoption of electronic health records in the US.” *Information & Management*, 53, no. 5 (2016) 570.

Shubayli, Miral Yahya Ahmed, Fatmah Ibrahim Mousa Kamili, and Bayan Hamad Ail Aashwa. “Roles and responsibilities of medical records staff in healthcare settings.” *Tec Empresarial*, 6, no. 2 (2024) 664.

Taiwo Adedeji, Hamish Fraser, and Philip Scott. “Implementing electronic health records in primary care using the theory of change: Nigerian case study.” *JMIR Medical Informatics*, 10, no. 8 (2022) e33491.

Tanwa Bada, Bamigboye, and Osundina. “Assessment of information security in the use of electronic health records management.” *Adeleke University Journal of Science*, 1, no. 1 (2022) 38.

Taylor, Allyn Lise. “Making the World Health Organization work: A legal framework for universal access to the conditions for health.” *American Journal of Law & Medicine*, 18, no. 4 (1992) 301.

Tom, Seymour, Dea Frantsvog, and Tod Graeber. “Electronic health records (EHR).” *American Journal of Health Sciences*, 3, no. 3 (2012) 201.

Tosin Clement, Callistus Obunadike, Darlington C. Ekweli, Oluomachi E. Ejiofor, Oluwadamilola Ogunleye, Simo Sevidzem Yufenyuy, and C. J. Obunadike. “Cyber analytics: Modelling the factors behind healthcare data breaches for smarter security solutions.” *International Journal of Advance Research, Ideas and Innovations in Technology*, 10, no. 1 (2024) 50.

Velthoven Van, Michelle Helena, Carlos Cordon, and Goutam Challagalla. “Digitization of healthcare organizations: The digital health landscape and information theory.” *International Journal of Medical Informatics*, 124, (2019) 49.

Vernon Weeks, Richard. “Electronic health records: Managing the transformation from a paper-based to an electronic system.” *Journal of Contemporary Management*, 10, no. 1, (2013) 140.

Williamson, Steven, and Victor Prybutok. “Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare.” *Applied Sciences,* 14, no. 2 (2024) 675.

Unpublished Dissertations

Adekunle Adewumi. *“‘Adequate protection’: an analysis of Nigeria’s data protection laws within an emerging global data protection framework”*. (Diss. 2022).

Ali GAGA, Thomas. *"A comparative study of data protection laws & policies: a case study of Nigeria."* (2022).

Ambrose Ojadale Attah.. Implementing an electronic health record in a Nigerian secondary healthcare facility: Prospects and challenges. (Diss. UiT The Arctic University of Norway, 2017). 12

Friday Ojonugwa, Agbo, Dr Gwom, and Solomon Gwom."The role and challenges of the National Agency for Food and Drug Administration and regulation of alternative medicine in Nigeria." (World Health 2021) 25.

Funnell, Sue, and Patricia Rogers. *Purposeful program theory: Effective use of theories of change and logic models*. (John Wiley & Sons, 2011).

Gbenro, Victor. Exploring the impact and roles strategic government leadership plays in adoption and use of eHealth in low resource countries: A case study of the medical and dental council of Nigeria as a professional health regulatory agency. (Diss. 2018).

Ibrahim Shehu. *Acceptance of Electronic Health Records for Improving Quality of Health Service Delivery: A Case Study of Aminu Kano Teaching Hospital Kano State, Nigeria*. (Diss. School of Computing and Information Technology, 2016).

Idoko, Benjamin. *"Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria."* (Magna Scientia Advanced Research and Reviews 2024).

Immanuel Kant, *The Metaphysics of Morals: The Metaphysical Elements of Justice; Translated, with an Inroduction by John Ladd* (Indianapolis: Bobbs-Merrill, 1965) xxix.

Jacquelyn O'herrin, Norman Fost, and Kenneth Kudsk, "Health Insurance Portability Accountability Act (HIPAA) regulations: effect on medical Health Insurance Portability and Accountability Act, 1996.

Johan Hansen. *"Assessment of the EU Member States' rules on health data in the light of GDPR."* (2021).

Ojadale Attah, Ambrose. *"Implementing an electronic health record in a Nigerian secondary healthcare facility. Prospects and challenges."* (2017): 5.

Olalekan Bello, and Cecile Ogufere. *"The Emerging Artificial Intelligence Legal-Judicial System's Interface: Assessing the State of Nigeria's Judicial System's Readiness for a Revolution."* (2024):6.

Prof. Onyemelukwe Cheluchi, and Dotun Bhadmus. *"Nigeria Data Protection Act 2023: relevant provisions for health care delivery in Nigeria."* Health Ethics and Law Consulting, Lagos (2024).

Randolph, Stetson Jay. *Identifying the Role of Healthcare Leaders in Protecting Sensitive Information Within Their Sector*. (Diss. National University, 2024).

Reza Faisal, Jose Prieto, and Stephen Julien *'Electronic Health Records: Origination, Adoption, and Progression'*, (2020) *Public Health Informatics and Information Systems* 188.
Semantha, Farida Habib, *"A conceptual framework to ensure privacy in patient record management system."* (2021): 165667.

INTERNET SOURCES

Kenneth Einar Himma, Legal Positivism. *Internet Encyclopeadia of Philosophy*. Available on https://iep.utm.edu/legalpos/#:~:text=Legal%20positivism%20is%20a%20philosophy,%2C%20reason%2C%20or%20human%20rights. Last Accessed 25 July 2025.

Kenneth Einar Himma, Legal Positivism. *Internet Encyclopeadia of Philosophy*. Available https://iep.utm.edu/legalpos/#:~:text=Legal%20positivism%20is%20a%20philosophy,%2C%20reason%2C%20or%20human%20rights. Last Accessed 28 July 2025.