LEGAL CONSIDERATIONS FOR ELECTRONIC MEDICAL RECORDS IN NIGERIA*

Abstract

Medical personnel in both public and private healthcare facilities are legally mandated to document all aspects of their patients' medical records, including diagnosis and treatment plan. Patient data documenting is still vital for promoting efficient patient care, and it is even required by law. Section 25 of the National Health Act, 2014.Section 25 of the National Health Act 2014[1] *requires that medical facilities maintain records of every patient who comes in. Health records often contain information about a person's vital signs, medications, family history, treatment history, medical directives, test results, consent documents, current medical issues and diagnosis, therapies, and progress notes.*[2] *The purpose of this essay is to examine existing Nigerian jurisprudence on the issue of electronic medical records and to draw a lesson or two from other countries. This article is fundamentally on the field of law. The research methodology used is doctrinal. As a result, main and secondary legal sources are used, such as statutes, cases, law books, international conventions, journals, and the internet.*

Keywords: Electronic, Medical Records, Legal Considerations, Nigeria

1. Introduction

The efficacy of a nation's healthcare delivery system is largely determined by its capacity to offer its citizens affordable, high-quality healthcare. Therefore, it is impossible to overestimate the significance of hospitals to a nation's healthcare delivery system. Medical records are essential for delivering high-quality medical treatment, and high-quality healthcare data is essential for the planning, creation, and maintenance of optimal healthcare. Patients' medical histories are documented in case notes, sometimes known as medical records. These are the handwritten or digital records that medical professionals produce and maintain that contain patient-specific information. Previously, doctors physically transported patient data between providers and maintained patient medical records on paper sheets. A rising number of hospitals and doctors' offices worldwide have already switched to digital patient records.

2. Purpose of Medical Records

Medical records can be used for a variety of purposes, three of which are relevant to this case. First, they document the patient's medical history, which includes examinations, diagnoses, and treatments. All healthcare professionals involved in a patient's care, as well as any new providers who take over later, must be aware of this information. The records include the diagnosis and recommended course of treatment from the patient's medical examination, as well as other relevant information. The medical personnel caring for the patient may alternate positions. This knowledge is vital since it will relieve previous and future healthcare practitioners of the need to rely on memory. One of the main reasons for maintaining current medical records is to guarantee that the patient receives ongoing care. Second, the data may be useful for research and could serve as the basis for investigating the patient's family, which is useful when there are hereditary diseases or people with similar characteristics. Third, for legal reasons including verifying health, injury, infection, and other claims, medical records could be required. Medical information is used by employers, schools, embassies, and numerous other organizations to grant jobs, admittance, visas, and other advantages. Because they can help with decision-making, medical records can also be used as a barometer by insurance companies to decide how much insurance coverage they can offer a patient or how much the patient should pay. A patient's medical records may demonstrate that his claims that his health condition was caused by a vehicle accident, a workplace injury, or anything similar are incorrect because the symptoms existed prior to the incident that is the basis of the patient's compensation claim. Good medical records are required for health practitioners to defend against a complaint or accusation of clinical negligence because they provide insight into the clinical judgment utilized at the time. Records acceptable for legal use are usually sufficiently thorough to ensure continuation of treatment.

3. Paper Based Medical Records

Paper-based medical records have long been utilized by Nigerian healthcare professionals. Increased information sharing, complex financial and legal issues, biomedical knowledge, the requirement for continuous care, and medical errors related to handwritten notes have made the paper-based method of clinical documentation inadequate. Other disadvantages include

***By Ugonna Sharon IHEKORONYE, LLB, BL, LLM, PhD Candidate**, Babcock University, School of Law & Security Studies, Iperu-Campus, Ogun State, Nigeria. MICMC, Lecturer, School of Law & Security Studies, Babcock University, Iperu-Campus Ogun State, Nigeria; Head of Chambers of Olumuyiwa Obanewa & co, opposites Sagamites Club, Sagamu Ogun State, Nigeria, Email: ihekoronyeu@pg.babcock.edu.ng, Tel: 08062085029.

***Chidinma Chizuru AKPARANTA, LLB BL, LLM, PhD Candidate,** Lecturer, Adeleke University, Ede. Osun State, Email: chyzranta@yahoo.com, Tel: 08132661687

***Olubukola OLUGASA**, Professor of Law, School of Law and Security Studies, Babcock University, Iperu-Campus Ogun, Nigeria, ACIS, ACIArb, Notary Public, Email: olugasao@babcock.edu.ng

***Osho Oludotun OLANIYI**, **LLB, BL, LLM, PhD Candidate**, Babcock University School of Law and Securities Studies, Nigeria, Managing Partner at Kola Abiri & Co. Plot 18 Goshen Estate, Elliot, Ishaga – Lagos State. Email: dotunosho@gmail.com, Tel: 07067736806

[1] National Health Act, No. 8 of 2014.

[2] Digital Health Folio 3 'The 10 Components of a Medical Record in a Hospital', available at https://digitalhealth.folio3.com/blog/10-components-of-a-medical-record/ accessed on 25th January, 2024.

the fact that it may not have enough physical space to store the cards in the event of a big patient population, that handwriting may vary from person to person, and that it may be vulnerable to termite or other infestations. Patients may become aware of private information and wait longer to obtain patient information when they must transfer these paper-based data across medical units. Furthermore, some individuals have several registrations with different healthcare providers, and hospitals, labs, or other physicians never see their information. As a result, information becomes diffused, causing disruptions, delays, and errors in patient treatment. Most of the time, patients do not have access to accurate and reliable information that they may use to meet their needs. Medical facilities sometimes only preserve paper records of their patients. Abdulkadir et al. demonstrated how erroneous requests might limit the value of paper-based medical data in Nigeria. It was also discovered that some records contained unreadable handwriting and cryptic abbreviations. Many of Nigeria's public tertiary teaching hospitals lack proper standards for preserving, protecting, and archiving patient medical records. Referral care may have a negative influence on patients.

4. Electronic Medical Record (EMR)

Electronic health records, often known as electronic medical records, or EHRs, have become more widely used. An electronic medical record, or EMR, is a longitudinal health record that contains entries made by healthcare providers at many sites where care is provided. Setting goals, planning patient care, documenting the delivery of care, and assessing the outcomes of that care are its primary uses. It includes information about what the patient needs from different medical specialists during a care episode.

Functionalities of the Electronic Medical Record (EMR)

A committee of the Institute of Medicine of the National Academies in the United States has identified eight essential care delivery functions that electronic health record systems should be able to carry out in order to promote increased safety, quality, and efficiency in the delivery of healthcare. They include:

Health information and data: In order for physicians and other healthcare professionals to make well-informed clinical decisions, specific patient data must be incorporated in an EMR. Therefore, EMR systems with defined datasets that include things like medical and nursing diagnoses, a medication list, allergies, demographics, clinical narratives, and laboratory test results can guarantee improved access to at least some types of information needed by care providers at the right time.

Results management: Through faster access to computerized results at their convenience, the practitioner may identify and address medical issues more rapidly, improving efficiency and patient safety by reducing waiting times.

Order entry/Order management: It allows medical practitioners to input instructions into a computer rather than writing them down for things like prescription drugs, lab work, radiography, and physical therapy.

Clinical decision support: It assists the healthcare professional in making decisions about the patient's care by providing the most up-to-date information about a medicine, comparing a patient's medication allergy, and sending out alerts for drug interactions and other possible patient issues that the computer has detected.

Electronic communication and connectivity: Communication between care partners, including lab, pharmacy, and radiology, should be made possible by EMR systems.

Patient support: Patient education is possible using EMR systems. The management of chronic illnesses has been significantly improved by patient education.

Administrative processes: Electronic scheduling tools for appointments, inpatient and outpatient procedures, and hospital admissions should be included in EMR systems. Patients will receive better, faster service as a result, and healthcare companies will become more efficient.

Reporting and Population Health Management: By making it simpler to gather standardized, systematic data in a format that can be shared across several healthcare organizations, EMRs can enhance reporting and surveillance. This can help public health organizations improve population health outcomes by helping them monitor, prevent, and control disease more effectively.

The Electronic Medical Record (EMR) provides various benefits to both consumers and healthcare practitioners. These advantages include clear and understandable documentation, improved data protection and security, interoperability, which allows for seamless sharing of medical records between healthcare providers, and ease of processing, retrieval, and access. The electronic medical record alternative eliminates the storage concerns associated with paper-based records. However, the main theme of this essay is the unique legal concerns that occur when healthcare facilities and their clients migrate to electronic records.[3] Patients' key legal concerns about their health data are ownership and administration of the data, availability and accessible, privacy, confidentiality, security, and integrity.

The Benefits of an Electronic Medical Record

Electronic medical records (EMR) are widely accepted in industrialized nations due to their advantages over paper records. This includes improve patient safety and quality of care. Efficiency is a significant advantage of an electronic information system. 'Doctors will have immediate access to potentially life-saving data, including lab test results, patient histories, and a list of prescribed medications,' according to a virtual system. Electronic document storage could improve departmental collaboration, resulting in increased productivity and faster emergency response. Similarly, by using computerized prescription entry, anticipating drug interactions and alerting healthcare providers, assisting clinicians in reconciling

[3]Aderibigbe T. O., Sodipo B., 'Patient's Medical Records, Privacy and Copyright in Nigeria: On-Going Research' available at https://www.law.uwa.edu.au/data/assets/pdf_file/0005/3052724/5.-Titilayo-O.-Aderibigbe-and-Bankile-Sopido.pdf accessed on 30th May 2023.

patients' medications, and maintaining an accurate and comprehensive medical record, the EMR can directly lead to improved patient safety by reducing medication errors in hospitals. Electronic records will also encourage individuals to participate more actively in their medical care by making lab tests and other records available online and providing electronic links to further information about their medical conditions. Because of the vast volume of patient information on paper and the current lack of a central storage system, most medical records are made up of multiple paper files stored in different locations. The paper method has frequently produced 'inaccurate, incomplete, untimely, fragmented, duplicative, and poorly documented' information. An electronic health care information storage system may minimize the inefficiencies and accuracy of traditional paper storage systems by making it easier to collect, organize, retain, and transmit personal information.

Improve care coordination and communication: The EMR allows numerous clinicians to see a patient consecutively, making the most recent information instantaneously available to all of them. Healthcare professionals have instant access to diagnostic tests and assessments performed by other clinicians. An EMR allows doctors to better coordinate and track patient care across offices and facilities. Clinicians from various professions and disciplines collaborate on patient outcomes to improve overall care, particularly chronic care management. Furthermore, rather than requiring many appointments, the approach allows patients to have their treatments, such as office visits, testing, surgery, and hospital visits, scheduled and coordinated at a single visit.

Cost reduction is another benefit: Costs will undoubtedly fall as a result of increased production and fewer issues with information retrieval and storage. When it comes to providing better medical care at a lower cost, numerous doctors who have worked with electronic records have found that the system works well for them. A reduction in malpractice premiums is another cost-saving benefit. Because electronic documentation of patient progress and visits can provide a strong defense against allegations of poor care, several insurance companies have reduced malpractice premiums by up to 10% based on the adoption of electronic medical records. The benefits of electronic medical records present significant opportunities in the health care sector. This has now become a high priority internationally.

Improved ability to conduct research: The availability of electronically recorded data for EMR systems will make it easier to uncover evidence-based best practices and conduct quantitative trend assessments. For example, the EMR frequently contains the data required for a study, therefore a major percentage of the data needed for research data collection is actually a result of routine clinical record keeping. De-identified EMR data might be merged into larger data repositories, allowing researchers to conduct studies to promote public health, medical understanding and patient safety.

Challenges of EMR implementation

The challenges experienced by wealthier nations while deploying EMRs differ slightly from those confronted by disadvantaged nations. Three major factors will be used to show the EMR challenges that developing countries such as Nigeria confront. They encompass political, human, and infrastructure issues.

Infrastructure issues

- Poor power supply
- According to the UK Department of Health, electricity is the 'most vital of all infrastructure's services,' as it is required for most other services to work. This demonstrates how vital power is in the delivery of healthcare. Nigeria now has a limited and unreliable electricity supply. The nation's limited electrical generation has resulted in insufficient power supply for general hospitals. To compensate, hospitals have turned to alternate energy sources such as solar panels and generators.
- Poor internet connectivity and availability.

Previous studies suggested that the bulk of Nigeria's suburban areas' expensive and poor internet connectivity would prohibit the EMR from being adopted, as a large bandwidth is required to analyze the EMR. Telemedicine and other real-time diagnostic support and training programs are among the most promising health applications for rural communities; nevertheless, their implementation has been impeded by a lack of low-cost bandwidth and connectivity. While mobile networks provide internet access in Nigeria's suburbs, respondents reported that the service is often inconsistent. Open protocols such as WIFI offer a reliable, inexpensive, and accepted alternative for rural wireless networks. The technology for ICT is poor. The electronic health record's rollout will be delayed by a lack of suitable technology.

Human factors

- Non-clinical and non-medical professionals lack adequate computer skills. Many non-clinical and non-medical healthcare professionals in ordinary hospitals lack basic computer operation and use skills. If qualified people must be hired in order to install the system, present employees may lose their jobs because the majority of them may be unable to learn the skills needed to operate the new system.
- Low level of awareness on eHealth
- Telemedicine is not widely accepted. Many healthcare personnel, particularly those in the records department, are still adjusting to the idea of utilizing computers to provide healthcare, and many are unaware that patient information can be saved electronically. This is because public hospital records departments are significantly understaffed with trained workers.
- Resistance from staff
  Hospital staff who are afraid of losing their jobs may battle against the implementation and create bottlenecks; for example, records department staff may be let go, and those who feel their jobs are at risk are likely to fight against

it. Furthermore, those who would be negatively impacted would do every effort to prevent the implementation, including lobbying the government through their union organization.

Political issues

- Poor administration

Politicians who run the government and take decisions on budgetary allocations are most times not in tune with advances in healthcare and often require competent advisers to recommend and push for the implementation of such novel ideas.

- Corruption

Corruption is one of the challenges. It manifests most times in the form of non-execution of awarded contracts or supply of sub-standard equipment. Other times, in their bid to make profit, the contractors cut corners and deliver outdated equipment to the hospitals thus making the hospital a dumping ground. This equipment begins to malfunction within a few months of installation leading to high cost of maintenance.

- Financial constraints

This was identified as one of the major challenges as General Hospitals, and indeed all government hospitals are grossly underfunded. The scarce resources have resulted in the inability to maintenance existing infrastructure and equally invest in new ones.

Legal Concerns

The major legal concerns for patients in relation to their health data revolve around ownership and control of the data, availability and accessibility, privacy, confidentiality, security and integrity of the data.

***Ownership and Control*:** Acknowledging that the patient against whom the record was generated in order to provide healthcare is the lawful owner of the information included in the record is the first step in determining who owns a health or medical record. However, as it is required by law and necessary to optimize healthcare, the record is under the responsibility of the medical professional.[4] When the ownership issue is examined from the perspective of privacy and data security, it is clear that the healthcare provider has control. But the 2023 Data Protection Act[5] guarantees that the data subject's rights—which include the right of access and the right to be erased—limit the aforementioned 'control' [6] etc., on the patient, who is the data subject in this instance. The NDPR Implementation Framework requires data controllers to provide procedures and systems that make it easier for patients to access and request data, as well as procedures that allow patients to swiftly and economically move (port) data to another platform. In order to provide care, the healthcare provider must have possession and control of the records; however, data privacy standards require that the patient or healthcare user have access to personal data and health records, among other rights. Patients in the United States have ownership rights to their health data, according to New Hampshire state statutes. However, in Nigeria, neither party has a clear ownership stake.[7] However, there is no distinct division of ownership reposed in either party in Nigeria.

Confidentiality: Confidentiality in healthcare is a critical concern, and electronic medical records are widely seen as having this benefit. Traditionally, a professional obligation in medical practice has been to safeguard the confidentiality of a patient's personal health information, unless the patient expressly agrees to divulge the information or there is another recognized legal justification. This derives from the Hippocratic Oath, which requires healthcare workers to maintain secrecy. Confidentiality is a fundamental principle of medical practice, and it is legally recognized as privileged communication between two parties in a professional relationship. The National Health Act of 2014 emphasizes the importance of a patient's right to confidentiality. Section 26(1) of the National Health Act states, 'All information concerning a user, including information relating to his or her health status, treatment, or stay in a health establishment, is confidential.' This highlights the importance of protecting the privacy of health-related information, both ethically and legally. Section 26(2) specifies when health records may be disclosed, including when the public's health is at risk and the user or patient has given written consent for disclosure, when a court order or other legal condition requires it, and in other cases.[11]

Additionally, as stated in Section 27 of the Act, medical personnel or professionals who have access to a patient's medical records may, in the course of their regular duties, disclose that patient's personal information to any other person, healthcare facility, or other third party as needed for any legal purpose, so long as doing so serves the patient's best interests.[12] According to Section 16 of the Freedom of Information Act of 2011, a public institution has the right to reject an application for information that is protected by the client privilege of health workers. This clause emphasizes how important confidentiality is. Section 25(f) of the Data Protection Act, 2023, imposes similar obligations on data controllers and processors, stating that sufficient organizational and technical measures must be implemented to ensure the confidentiality, integrity, and availability of personal data. To avoid the potential problems that an electronic system may

[4] Laurinda B. Harman, Cathy A. Flite, and Kesa Bond, 'Electronic Health Records: Privacy, Confidentiality, and Security', available at https://journalofethics.ama-assn.org/article/electronic-health-records-privacy-confidentiality-and-security/2012-09 accessed on 25th April 2023.

[5] Data Protection Act, 2023.

[6] Section 35(b).

[7] Raj Sharma, 'Who Really Owns Your Health Data?' available at https://www.forbes.com/sites/forbestechcouncil/2018/04/23/who-really-owns-your-health-data/?sh=438761d56d62 accessed on 25st January 2024.

provide, the most important of which is the unjustified invasion of patient privacy, care must be taken to guarantee that a paperless system will keep patient information private and confidential.

Privacy and Security: As was already established, private information like drug addiction, infectious diseases, terminal illnesses, psychological disorders, and psychiatric treatments may be revealed from health records. This information could expose the data subject to many forms of unsolicited marketing, including product promotion, blackmail, and others.[8] Therefore, it is essential to ensure that the privacy of the data subject is protected. In the context of healthcare, privacy refers to a patient's right to control their own health information and to keep it private. Potential use and disclosure scenarios for a patient's protected health information are also covered. The Nigerian Constitution recognizes the right to privacy as a fundamental freedom. In addition to the constitutional provision and professional need, privacy law adds another level of legal protection and responsibility. The definition of privacy provided in *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors. v. NIMC* is the 'protection of personal information and personal data.' It is commonly interpreted to denote a situation in which there is no public awareness or disturbance. In addition, the Nigeria Data Protection Regulations, 2019 (NDPR) protect the Constitution's guarantee of privacy.[9] and the Data Protection Act, 2023 hence for data controllers in the healthcare industry, privacy is crucial. Under the Data Protection Act, health status-related data is categorized as sensitive personal data, even though information about an identified or identifiable natural person, including medical information, is considered personal data.

Security: A crucial element that includes both paper and electronic health records is healthcare security. Security includes safeguarding the digital and physical locations where medical records are stored. A security breach affects medical records as well as medical equipment. Security breaches in healthcare businesses can have a variety of negative effects, such as decreased patient trust, lost revenue, reputational damage, and fines from the government. As more records are being digitized, cyber-attacks are happening increasingly often in the healthcare sector. A patient's right to privacy may be violated in the event of an accidental data loss, an abusive or illegal use of privileges, a cyber-attack, or an unlawful disclosure. The NDPR states that data controllers and processors need to have plans to protect data security. Healthcare facility and establishment management is advised to use data encryption technologies, install firewalls, store data securely with limited access, and establish organizational policies for handling personal data (as well as other sensitive or confidential data). protect email systems and ensure that staff members are always improving their skills.[19] Furthermore, whenever data processing involves sensitive or highly personal data, relates to vulnerable or differently-abled data subjects, or involves health establishments considering the implementation of novel procedures or the use of cutting-edge technological solutions, data protection impact assessments are necessary to determine the privacy and security implications.[10] In accordance with Section 29 of the National Health Act, health establishments that hold user health records are required to put in place appropriate measures to guarantee that the management of those establishments has control over the installation of security measures to prevent unwanted access to the records and the system or storage facility used to keep them.

In addition, the Act stipulates that failure to carry out this duty will result in a fine of two hundred and fifty thousand Naira (D50,000), two years in prison, or both. The NDPR even goes so far as to require a duty of care from anybody who has been given or is in possession of a data subject's personal information. This means that in the event of a breach, healthcare facilities will have to make sure that their EMR (software-as-a-service) provider guarantees the security of patients' sensitive personal data. Encryption and password security measures, among other security standards, must be included in the software's design. After the EMR software is installed in the healthcare institution, healthcare practitioners are still accountable for making sure the system is properly monitored and gets regular maintenance and updates. They must follow sound data governance practices and stay up to date on developments in cybercrime. There has been strong opposition to the use of electronic health information systems including EMRs, despite their potential advantages. Electronic medical record storage is opposed on the grounds that it may seriously violate patient privacy. 'The electronic information revolution is altering the recording of health information to the point where disclosure may be as simple as pushing a button. According to the American Health Information Management Association, an average of 150 persons has access to a patient's medical records during a standard hospital stay. Many of those who have access have a valid need to read the record, but there are no laws governing who they are, what information they can see, and what they can and cannot do with patients' personal information once they have it. Furthermore, much of the sharing of medical information occurs without the impacted patient's knowledge. The security of medical information is a vital element. However, as medical records are incorporated into the electronic realm, things change. Courts may be unable to protect how and why documents are utilized.

5. Legal Framework for Privacy and Security in Nigeria's Healthcare Sector

Section 37 of the Federal Republic of Nigeria 1999 Constitution guarantees the right to privacy to all Nigerians. Although there isn't yet a general cybersecurity and data protection law in Nigeria, there are continuing legislative attempts and sector-specific frameworks in place to create one.

[8] Karen N. Brown, 'How Medical Data Sharing is Impacted by EU GDPR', available at https://www.volusonclub.net/empowered-womens-health/how-medical-data-sharing-is-impacted-by-eu-gdpr/ accessed on 25th January 2024.

[9] Nigeria Data Protection Regulations, 2019 (NDPR).

[10] See Paragraph 5.2 of the NDPR Implementation Framework, 2020 available at https://ndpb.gov.ng/Files/ImplementationFramework.pdf accessed on 25th January 2024

National Health Act (NHA) 2014: Nigeria's healthcare industry is mostly governed by the NHA. Furthermore, it provides sufficient safeguards for patients' right to privacy. As stated in NHA Section 26 (1), 'all information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is confidential.' The legal duty of confidentiality is enforced by the clause. As per Section 26(2) of the Act, there are specific limitations on the right. When a judicial order or other legal need necessitates its disclosure and the owner provides written authorization, health information may be shared, provided that withholding it would seriously endanger public health. In the same way, NHA Section 25 mandates that health records be kept accessible to patients. According to Section 27 of the Act, a user's health record may be disclosed to a third party, another healthcare provider, or professional on two legal grounds: first, if the disclosure is required for any justifiable reason within the regular course and scope of the person's duties; and second, if the user would benefit from the access or disclosure. The latter is comparable to establishing a legal basis based on vital interest.

Section 28 (1) allows a healthcare provider to view a patient's health record with the patient's agreement. This establishes consent as a legal basis. The clause also provides for the use of health records for research purposes with the patient's approval. Section 28 (2) states that the patient's or any other authority's authorization may be waived for the purposes of research, teaching, and studying if the research data contains no personally identifiable information. Section 29 requires the head of a healthcare facility to implement 'control measures to prevent unauthorized access to those records and to the storage facility in which, or system by which, records are kept'. This means that effective data governance and management practices are needed to guard against both online and offline data theft, loss, and illegal disclosure in addition to unauthorized access. According to this clause, infractions carry a two-year prison sentence, a N250,000 ($816) fine, or both. Falsification or alteration of records, destruction of records without authorization, re-identification of de-identified documents, unauthorized access to or interception of records are among the offenses.

Cybercrimes (Prohibition, Prevention, Etc) Act: Certain economic sectors are designated as Critical National Information Infrastructure (CNII) in Section 5 of the Cybercrimes (Prohibition & Prevention) Act 2015. The healthcare industry is classified as a National Critical Information Infrastructure under Part 7.5 of the National Cybersecurity Policy. Attacks on areas designated as important national infrastructure are illegal under the Act and are punishable by a minimum 15-year jail sentence without the possibility of a fine. The Act also lists further offenses that can have an impact on the industry. The Nigeria Computer Emergency Response Team (NgCERT), the government's coordinating center in charge of handling cyber incidents in Nigeria, must be notified of any cyberattack or threat, according to Section 21 of the Cybercrimes (Prevention and Prohibition) Act. Failure to report within seven days results in a fine of N2,000,000 ($6,535) and denial of internet connectivity. Underreporting remains a debilitating element in calculating the cost and scope of cybercrime, robbing the sector of shared common information. The NgCERT has developed an online portal for reporting incidents as an individual or an organization.

National Health Insurance Scheme Act (NHIS Act): Officials and other scheme workers are subject to a secrecy requirement established by Section 38 of the Act. Officials are required to maintain the confidentiality of any information they learn while performing their duties or while exercising their responsibilities. Only a court order or an arbitration board may receive access to the private data. A fine of at least N20,000 ($65) or two years in jail are the applicable penalties under Section 38 (2).

Freedom of Information Act (FOI Act): According to Section 16 of the FOI Act, a public entity has the right to reject a request for information that is protected by the client privilege of health professionals. The professional confidentiality responsibility is acknowledged and given legal support in this section.

Patients' Bill of Rights (PBOR): The Patients' Bill of Rights (PBOR) was recently released by the Consumer Protection Council (CPC). The purpose of the Bill is to guarantee that the nation has simple access to high-quality medical care. The Public Bill of Rights (PBOR) is a list of rights that are already included in existing legislation that was condensed into a pamphlet in order to raise public awareness. Remarkably, the bill acknowledged patients' rights to secrecy about their medical data and their privacy. In addition to the medical profession's professional duty of confidentiality, patients' freedom and right to privacy are further safeguarded by a legal responsibility.

6. International Best Practices for Electronic Medical Records: Lessons for Effective Implementation

Electronic medical records, or EMRs, are now a vital component of contemporary healthcare systems across the globe, facilitating better patient care, more effective healthcare delivery, and improved data management. Nigeria may gain important insights from global best practices in the areas of legal frameworks, interoperability, privacy, and security to guarantee successful adoption.

Legal Frameworks for EMRs:

United States: Standards for EHR interoperability, privacy, and security are established by the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Health Insurance Portability and Accountability Act (HIPAA), with a focus on patient rights and data protection.

Australia: The Personally Controlled Electronic Health Records Act (PCEHR Act) governs the creation, use, and disclosure of electronic health records while stressing patient control, privacy, and security.

Singapore: The goal of the National Electronic Health Record programs is to achieve nationwide interoperability by means of a centralized healthcare information repository that can be accessed by authorized healthcare providers.

Canada: Organizations are required by the Personal Information Protection and Electronic Documents Act (PIPEDA) to handle health information carefully, and it sets guidelines for data security, consent, and privacy.
Germany: The Federal Data Protection Act (BDSG) of Germany establishes stringent guidelines for the processing and management of health data, placing a strong emphasis on patient consent and security precautions to preserve their privacy.
United Kingdom: Guidelines for patient permission, data protection, and EMR security are provided by the Data Protection Act of 2018 and the National Health Service (NHS) Digital Code of Practice for Handling Information in Health and Care.

7. Conclusion

The full potential of electronic technology in the health care sector will not materialize unless privacy and confidentiality issues pertaining to electronic medical records are resolved. 'The lack of uniform national standards for regulating medical information hampers and reduces the effectiveness of administrative simplification,' yet 'technological advances have made new computer systems more reliable and secure than paper-based systems.' 'It is imperative that stronger laws address privacy concerns.' Tougher penalties for individuals who violate appropriate privacy practices must also align with stricter restrictions pertaining to the monitoring of who may have access to patient information. The cultural and constitutional cornerstone of personal privacy may be compromised by the switch from paper medical records to an electronic-based system if these crucial adjustments are not made. In addition, even while healthcare facilities play a major role in the conversation around health and medical data, EMR software providers also need to be brought to light. Software vendors are becoming important players in the healthcare industry as a result of the use of health technology. Therefore, start-ups and businesses that provide EMR software should pay special attention to data protection compliance. It is especially important to highlight the NDPR's self-reporting method for EMR software providers that work with healthcare facilities. In the same way, when creating, sustaining, and enhancing their software solutions, EMR firms need to keep in mind the legal factors mentioned above. Nigeria and other nations looking to create efficient legal frameworks, promote interoperability, and give privacy and security first priority will benefit from learning from international best practices in EMR implementation. Through the adoption of best practices from successful global implementations, nations may preserve patient privacy, enable smooth data interchange, enhance healthcare outcomes, and encourage moral research and data usage practices. The ongoing exchange of information and insights will eventually help progress electronic health records worldwide and improve healthcare systems everywhere.