

DATA BREACH IN HEALTHCARE SECTOR: LEGAL RESPONSIBILITIES AND ITS EFFECTS ON PATIENTS

Muslim Nasirudeen Ade*

Abstract

The recent hack on the Plateau State Contributory Health Care Management Agency (PLASHEMA) and the rapid rise in healthcare data breaches globally highlight the critical need for strong data security policies in healthcare institutions. This article investigates the serious consequences of data breaches on patient privacy and trust in the healthcare system. It focuses on legislative frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the Nigeria Data Protection Regulation (NDPR) for protecting patient data. The paper finds that despite these efforts, the current legal landscape is ineffective in discouraging frequent and large-scale cyber-attacks. This study proposes for stronger legislative frameworks, increased investment in security measures, and patient education to restore trust in healthcare data security. Furthermore, it investigates the issues encountered by the Nigerian healthcare system in combating data breaches among others.

Keywords: cyberattack, data breach, healthcare, patient privacy, regulatory framework, cybersecurity.

1.0 Introduction

* Senior Lecturer, General Studies Department, Oke Ogun Polytechnic, Saki, Oyo State.
Email: ajisefoni@gmail.com

2.0 Overview of Comparative Legal Framework for Laws Governing Data Protection in Selected Jurisdictions

2.1 The Nigerian Data Protection Act 2023

The Nigerian Data Protection Act 2023 is a major piece of legislation that governs the handling of personal data in Nigeria. It provides a comprehensive data protection and privacy framework that is consistent with international standards and addresses growing concerns about data security in the digital age. The Act is a critical step towards protecting personal data and improving privacy rights in Nigeria.¹⁵ The Act intends to encourage confidence in the digital ecosystem and promote responsible personal data management by setting clear principles and strong enforcement measures. As the digital ecosystem evolves, the Act provides a vital foundation for addressing data protection concerns in the twenty-first century. Data Controllers should appoint a Data Protection Officer (DPO) who would be accountable for maintaining internal compliance with the Act and other relevant data protection guidelines and acting as a liaison between the Data Controller and the regulatory agency.

2.1.1 An Overview of Key Provisions of the Nigerian Data Protection Act 2023

a. Scope and Applicability

The Act applies to all data controllers and processors operating in Nigeria, as well as those located outside of Nigeria who process personal data of

¹⁵ Babalola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) SSRN 4786872 <https://ssrn.com/abstract=4786872> accessed [76/7/2024]

Nigerian residents. This extraterritorial applicability ensures that data subjects are safeguarded no matter where their information is handled.

b. Data Processing Principles

The Act outlines several principles for the lawful processing of personal data, including:

- i. **Lawfulness, Fairness, and Transparency:** Data must be processed in a lawful, fair, and transparent manner.
- ii. **Purpose Limitation:** Data should be collected for specified, legitimate purposes and not further processed in a manner incompatible with those purposes.
- iii. **Data Minimization:** Only the data necessary for the purposes stated should be collected.
- iv. **Accuracy:** Personal data must be accurate and kept up to date.
- v. **Storage Limitation:** Data should not be kept longer than necessary.
- vi. **Integrity and Confidentiality:** Appropriate security measures must be in place to protect data against unauthorized access, alteration, or destruction.

c. Rights of Data Subjects

The Act grants data subjects several rights, including:

- i. **Right to Access:** Individuals have the right to access their personal data and obtain information about how it is being processed.
- ii. **Right to Rectification:** Data subjects can request the correction of inaccurate or incomplete data.
- iii. **Right to Erasure:** Individuals have the right to request the deletion of their personal data under certain circumstances.
- iv. **Right to Restriction of Processing:** Data subjects can request the restriction of data processing under specific conditions.
- v. **Right to Data Portability:** Individuals can request to receive their data in a structured, commonly used, and machine-readable format.
- vi. **Right to Object:** Data subjects have the right to object to the processing of their data on grounds relating to their particular situation.

d. Obligations of Data Controllers and Processors

Data controllers and processors are required to implement appropriate technical and organizational measures to ensure compliance with the Act. This includes conducting data protection impact assessments, maintaining records of processing activities, and appointing a Data Protection Officer (DPO) where applicable.¹⁶

e. Data Protection Authority

The Act establishes the Nigerian Data Protection Bureau (NDPB) as the regulatory authority responsible for enforcing data protection laws. The NDPB has the power to investigate data breaches, impose fines, and issue directives to ensure compliance.

f. International Data Transfers

The Act imposes restrictions on the transfer of personal data to countries outside Nigeria, ensuring that such transfers are subject to adequate levels of data protection. Data transfers are permitted only if the receiving country provides adequate protection or if specific safeguards are in place.

g. Penalties and Enforcement

Non-compliance with the provisions of the Act can result in significant penalties, including fines and sanctions. The NDPB is empowered to enforce compliance through investigations, audits, and the imposition of fines.

3.0 Legal Responsibility in Data Breaches - Protecting Patient Privacy

5.0 The Nigerian Healthcare System and the Fight for Patient Data Security

6.0 Overview of Specific Case Studies of Data Protection and Violation

8.0 The Way Forward

9.0 Conclusion and Recommendations

¹⁶ Babalola O, 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12(1) *International Data Privacy Law* 44