Patient Data, Real Liability: What the NDPA Means for Healthcare SMEs

Introduction

Healthcare providers handle some of the most sensitive personal information in Nigeria. From patient records and laboratory results to prescriptions and billing information, the collection and use of health data is now governed by the Nigeria Data Protection Act 2023 (NDPA) and the General Application and Implementation Directive (GAID).

For clinics, diagnostic centres, pharmacies, and other healthcare SMEs, data protection is no longer simply an administrative or IT concern. It is a legal and regulatory obligation that forms part of responsible healthcare governance, with significant compliance, financial, and reputational implications.

Key Highlights

- **Health data attracts enhanced protection:**

Medical records, prescriptions, laboratory results, and other patient information are classified as sensitive personal data under the NDPA and must be processed with enhanced safeguards.

- **Some healthcare providers must register with the NDPC:**

Healthcare organisations that qualify as Data Controllers or Data Processors of Major Importance are required to register with the Nigeria Data Protection Commission (NDPC). Knowing whether you cross that threshold is the first question, not an afterthought.

- **Data governance is now a regulatory expectation:**

Depending on the applicable classification, organisations may be required to appoint a Data Protection Officer (DPO), implement appropriate internal policies, and maintain effective data protection governance measures.

- **Compliance extends beyond consent:**

Healthcare providers are expected to implement appropriate security measures, maintain adequate records, report qualifying data breaches within the prescribed timeframe, and comply with applicable regulatory reporting obligations.

What This Means for Stakeholders

- **For healthcare SMEs:**

Patient data protection should be integrated into everyday clinical operations. Consent procedures, record management, staff access controls, and internal processes should be reviewed to ensure compliance with the NDPA.

- **For healthcare business owners**:

Data protection should form part of broader corporate governance and risk management, not a side issue. Regulatory non-compliance may expose businesses to investigations, financial penalties, and lasting reputational damage.

- **For health-tech businesses:**

As healthcare services become increasingly digital, providers should ensure that electronic medical records, cloud storage solutions, mobile applications, and third-party service providers comply with applicable data protection requirements.

- **For patients:**

Patients should expect more- clearer consent processes, better protection of medical records, and greater accountability in how healthcare providers collect, store, and share their personal information.

- **For the healthcare sector:**

Strong data governance is becoming an essential component of regulatory compliance, patient confidence, and sustainable healthcare delivery.

The Road Forward

The NDPA marks a shift from viewing patient information as merely confidential to recognising it as a regulated asset requiring ongoing governance and oversight. For healthcare providers, compliance is no longer a one-off exercise but an integral part of delivering healthcare services responsibly.

Healthcare SMEs should review their data protection frameworks, strengthen internal governance, and ensure that patient information is managed in line with current regulatory requirements. Patients should also understand their rights, including how their health data is collected, used, stored, shared, and protected.

For guidance on NDPA compliance, healthcare data governance, Data Controller or Data Processor of Major Importance classification, or redress for data privacy breaches, contact info@scp-law.com or visit www.scp-law.com.