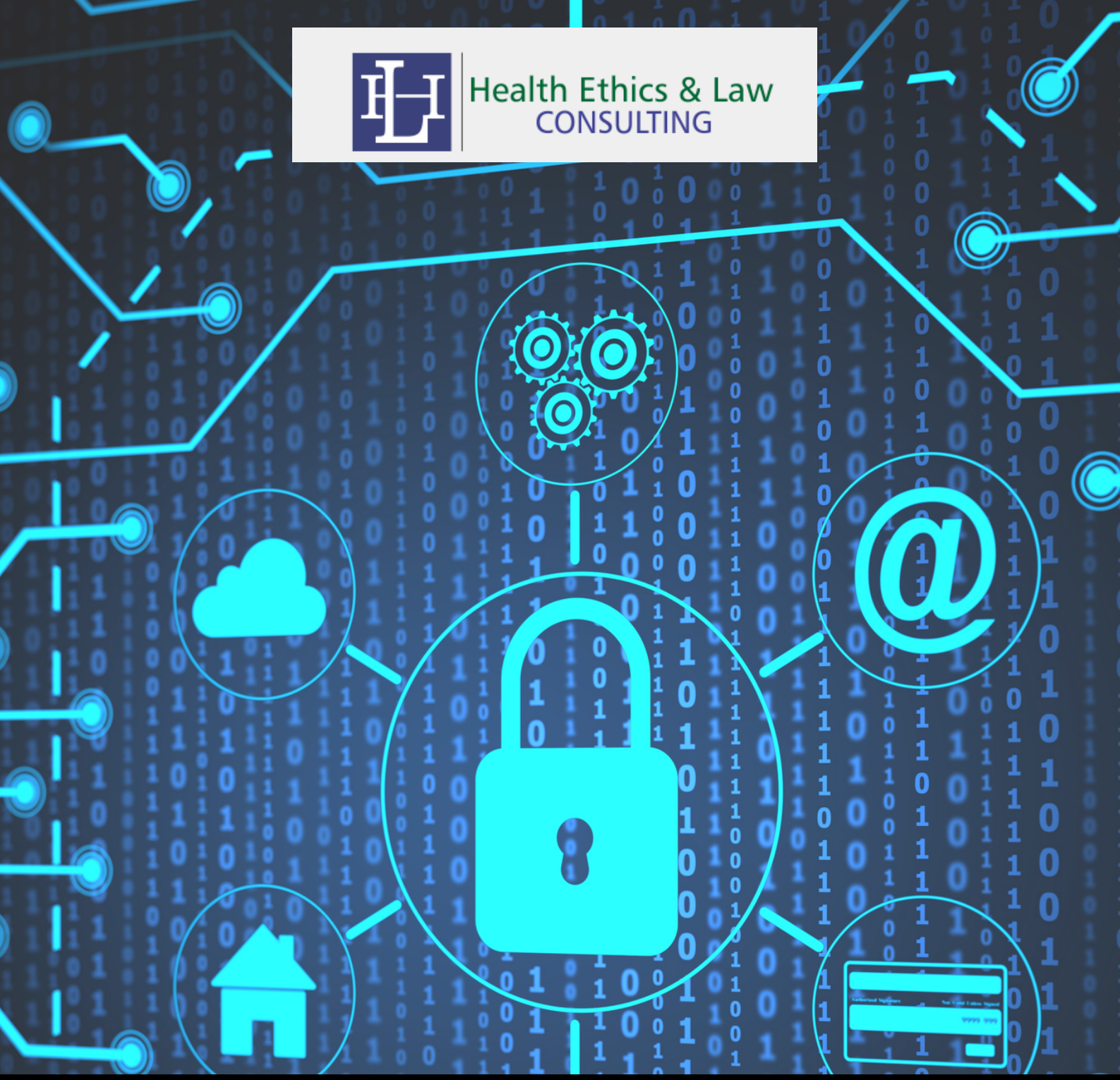

NIGERIA DATA PROTECTION ACT 2023: RELEVANT PROVISIONS FOR HEALTH CARE DELIVERY IN NIGERIA

1.Introduction

The Nigeria Data Protection Act 2023 (NDPA) was signed into law in Nigeria. The Act provides for the protection of personal data. It is the first law enacted to address specifically the protection of personal data in Nigeria after repeated attempts by past administrations to enact legislation on data protection. These attempts led to the issuance of the Nigeria Data Protection Regulations 2019 by the National Information Technology Development Agency. Although only subsidiary legislation, the Nigeria Data Protection Regulations laid the basic foundation for protecting personal data in an era where protecting personal data has become more critical.

The Nigeria Data Protection Act seeks to ensure uniformity in the processing of personal data, while also safeguarding the fundamental human rights, freedoms, and interests of data subjects as provided for under the 1999 Constitution, and providing remedies for breach of data.[1]

The Act has implications for different sectors of the economy. One key sector to consider is the health sector. The health sector is composed of myriad actors who deal with a variety of data, such as collectors and processors. These include public and private hospitals, pharmacies, laboratories, public health insurance schemes, health maintenance organisations, and clinical research organisations. It also includes government agencies such as the National Public Health Institute or surveillance agencies working as part of the government, health regulatory bodies, and professional health regulatory agencies. Furthermore, it includes digital healthcare businesses providing electronic medical records (EMR) solutions, telemedicine virtual consulting platforms, and other services. Each of these entities has many opportunities for collection, use, processing, and storage of data. Each of these has obligations with respect to the protection of personal data. It is therefore critical to identify and understand the implications of the Act on the operations of these actors. This will not only help clarify roles and responsibilities but ultimately improve health outcomes while protecting patient/user information.

[1] Section 1 of the NDPA.

2. Overview of the Nigeria Data Protection Act

Interestingly, the Nigeria Data Protection Act does not repeal the Nigeria Data Protection Regulation 2019 (NDPR). Section 64 (2)(f) provides an avenue for the continuing existence of the NDPR, expressly providing that all regulations, rules, etc, made by the Nigeria Information Technology Agency or the Nigeria Data Protection Bureau on data protection continue to remain in effect until they have been repealed. Though the Nigeria Data Protection Regulations 2019 remain in force, where there are inconsistencies between the provisions of the Act and the Regulations, the Act shall take precedence.[2] This goes without saying that provisions of the NDPR that are not inconsistent with the provisions of the Act remain applicable and enforceable.[3]

The Act also makes provisions relating to the processing of personal data, principles of processing personal data, rights of data subjects,[4] the appointment of data protection officers [5], and data privacy impact assessment in cases where the processing of personal data will likely result in a breach of personal data of data subjects, etc.[6] Data controllers/ processors are required to establish a lawful basis for processing personal data, some of the lawful bases provided by the Act include: When the data subject has given and not withdrawn consent, For compliance with a legal obligation to which a data controller/processor is subject, [7] For the performance of a task carried out in the public interest.[8]
Data controllers/processors are also required to process personal data following laid down principles for processing personal data, some of these include the requirement that: The data must be processed in a fair, lawful transparent manner; The data collected must be for a legitimate purpose, and should not be processed in any manner incompatible to that purpose; The processing of the data must be adequate, relevant and limited to the minimum necessary, etc[9]

3. Selected Relevant Provisions of the NDPA on Health

The Act makes specific provisions for personal data processing in relation to public health and health care. We set out some of these provisions below.

---

[2] Section 63 of the NDPA
[3] The provisions of the NDPR as it relates to the qualities of a DPO (though not mandatory) remains applicable
[4] Section 34-38 of the NDPA
[5] Section 32 of the NDPA
[6] Section 28 of the NDPA
[7] Court Order, for instance can fall under this ground
[8] Section 25 of the NDPA
[9] Section 24 of the NDPA

i. Exemption from obligations under Part (V) of the Act, of Data Processed During Pubic Health Emergencies by Competent Authorities.

The NDPA provides for certain exemptions from the lawful basis governing the processing of data. Key amongst them is data processed by competent authorities for the purpose of prevention or control of national public health emergencies, [10] such as the COVID-19 pandemic, or the epidemics of Lassa Fever and Cholera faced almost yearly in Nigeria. The competent authority is defined under the interpretation section to mean "Government of the Federal Republic of Nigeria or any Foreign Government, or any State government, statutory authority, government authority, institution, agency, department, board, commission, or organization within or outside Nigeria exercising either executive, legislative, judicial, investigative, regulatory, or administrative functions."[11] This would include agencies such as the Nigeria Centre for Disease Control and Prevention which, in the exercise of its mandate and under the provisions of the Act, can lawfully process data free from certain obligations under Part V of the Act. Some of the obligations exempted include; The burden of proof placed on data controllers when there is a question, as regards whether consent was freely or intentionally given,[12] The requirement to undertake a data privacy impact assessment, where the processing of personal data will likely result in a high risk to the rights and freedom of data subject,[13] The requirement to obtain consent from a parent or legal guardian of children under the age of 18 years,[14] The right of data subject.[15]

Processing of personal data by competent authorities in times of public health emergencies is however subject to certain restrictions, which the competent authority must comply with. These include; Section 24 which deals with (Principles of Personal Data Processing), Section 25 which deals with (Lawful Basics of Personal Data Processing), Section 32 which deals with (Data Protection Officers) and Section 40 which deals with (Personal Data Breaches). These sections will apply to the processing of personal data by competent authorities. For example, a lawful basis for processing personal data must be established. Such lawful basis for processing personal data during public health emergencies may include grounds of public interest. The competent authority is also required to appoint a data protection officer, and in line with section 40 report any personal data breaches to the Commission within 72 hours of becoming aware of the breach.

---

[10] Section 3(2)b of the NDPA
[11] Section 65 of the NDPA
[12] Section 26 of the NDPA
[13] Section 28 of the NDPA
[14] Section 31 of the NDPA
[15] Section 34-38 of the NDPA

ii. The requirement For Registration of Data Controllers of Major importance

The Act introduces a certain class of data controllers and data processors different from normal data controllers (DC) and data processors (DP) named "Data Controllers of Major Importance and Data Processors of Major Importance"[16] (DCMIs and DPMIs). The DCMIs and DPMIs are required to register with the Commission[17] and are subject to stricter fines than those imposed on regular DCs and DPs. DCMIs and DPMIs are subject to a fine of over 10,000,000 or 2% of their annual gross revenue in the preceding financial year, whichever is higher,[18] while DCs and DPs are subject to a fine of over 2,000,000 or 2% of their annual gross revenue in the preceding financial year, whichever is higher.[19] The fine kicks in when they are adjudged by the Commission to have violated the Act or any subsidiary legislation. Regulations fall under subsidiary legislation which data controllers and data processors should avoid breaching.

Data Controllers of Major Importance and Data Processors of Major Importance are not fully defined, with the Act creating room for the Commission to do so by regulation. [20] The Commission in February 2024, clarified who constitutes 'data controllers of major importance and data processors of major importance through a Guidance Notice. According to the Guidance Notice, [21] a data controller or data controller will be deemed to be of major importance if it (a) processes the personal data of more than 200 (Two- Hundred) data subjects within the span of six months, or (b) carries out ICT services through the use of any digital device having storage capacity, and belonging to another individual, or (c) processes personal data either as an organization or a service provider in the Financial, Communication, Health, Education, Insurance, Export sectors etc. [22] Data Controllers or Processors who are under a fiduciary duty with a data subject for which the duty of keeping confidential information is crucial are also regarded as Data Controllers or Processors of Major Importance. [23]

---

[16] Section 44(1) of the NDPA
[17] The Act requires the DCMIs and DPMIs to register with the Commission within 6 months after the commencement of the Act or on becoming a data controller of major importance or processor of major importance
[18] Section 48(3)(a) and (4) of the NDPA
[19] Section 48 3(b) and (5) of the NDPAi
[20] The Act defines data controller or data processors of major importance to be " data controller or data processors of major importance domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other classes of data controllers or data processors that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate". See Section 65 of the Act
[21] paragraph 1 of the Guidance Notice
[22] https://ndpc.gov.ng/Files/registration.pdf
[23] ibid

Reviewing the Guidance Notice, it seems fairly clear that most if not all healthcare stakeholders are likely to fall under data controllers of major importance (DCMIs) or data processors of major importance (DPMIs). At any rate, the majority of healthcare stakeholders will fall under (c) as organizations or service providers in the health sector who process personal data. Healthcare providers like telehealth companies, digital health businesses, hospitals, and other stakeholders like health insurance companies, among other healthcare entities, are required to register as DCMIs or DPMIs.[24]

Furthermore, the Guidance provides for registration by DCMIs and DPMIs, and to aid the registration process, classifies DCMIs and DPMIs into three categories [25]namely: Major Data Processing Ultra Level (MDP-UHL), Major Data Processing-Extra High Level (MDP-EHL), Major Data Processing-Ordinary High Level (MDP-OHL). Insurance companies which will include health insurance companies may be classified as Major Data Processing Ultra High Level (MDP-UHL) and are required to pay a non-refundable fee of N250,000 (Two Hundred and Fifty Thousand Naira) for registration.[26] The Ministry of Health as a ministry of the government, hospitals providing tertiary or secondary medical services are classified as Major Data Processing-Extra High Level (MDP-EHL) and are required to pay a non-refundable fee of N100,000 (One Hundred Thousand) for registration.[27] Primary Health Centres are classified as Major Data Processing -Ordinary High Level (MDP-OHL) and are required to pay a non-refundable fee of N10,000 (Ten Thousand Naira) for registration.[28] DCMI's and DPMI's in line with section 44(1) of the Act[29]and the guidance notice are required to register on or before the 30th of June 2024[30] failing which shall be deemed a default under the Act and liable to a penalty stipulated under the Act. [31] The penalties have been highlighted in this Article.

iii. Sensitive Personal Data: Exclusion of Sensitive Data Processed for the purpose of medical care.

The Act does not define 'health data.' However, it classifies health data as sensitive personal data. The NDPR, which was in place before the enactment of the Act mentions sensitive personal data and defines it as data relating to religious or other beliefs, sexual orientation,

---

[24] ibid
[25] Paragraph 2 of the Guidance Notice
[26] Paragraph 3(1)(a) of the Guidance Notice
[27] Paragraph 3(1)(c) of the Guidance Notice
[28] Paragraph 3(1)(e) of the Guidance Notice
[29] Act requires DCMI's and DMPI's to register within 6 months of the commencement of the Act or within 6 months of becoming a DCMIs or DPMIs
[30] Paragraph 3(2) of the Guidance Notice
[31] Paragraph 3(3) of the Guidance Notice

health, race, ethnicity, political views, trade union membership, criminal records, or any other sensitive personal information. [32] The NDPR also requires data controllers, and data processors to set up security measures to enable proper handling of sensitive personal data.[33] These provisions are by no means, exhaustive or even of broad coverage.

The Act, on the other hand, defines sensitive personal data to mean "genetic and biometric data, for the purpose of uniquely identifying a natural person, race or ethnic origin; religious or similar beliefs, such as those reflecting conscience or philosophy, health status, sex life; political opinions or affiliations, trade union membership, or other information prescribed by the Commission" [34] Thus data relating to health status, genetic data and biometric data (data identifying individuals) are protected under the Act as sensitive personal data. The Act attaches specific obligations to the processing of sensitive personal data. According to the NDPA, sensitive personal data should not be processed, except on specific grounds. Some of the specific grounds for processing sensitive personal data include: When consent has been obtained for processing sensitive personal data, and the same has not been withdrawn[35] When processing is necessary for compliance with social security or employment laws.[36]

Some specific grounds are particularly relevant for healthcare organisations. Healthcare entities can rely on the processing of personal data when it is necessary to protect the vital interest of the data subject when he or she is physically or legally incapable of giving consent[37]. This may apply in a situation where data is to be processed and the patient is unconscious. Other persons that fall under this ground include children, and in some cases, adults with mental illness or intellectual disability which affect their capacity to make decisions regarding their medical treatment. In all cases, the best interest principle shall prevail for the processing of sensitive personal data of this class of persons, with consent to be sought from guardian ad litem or supportive decision-makers. Sensitive personal data can also be processed for the purpose of providing medical care or community welfare[38] The Act also provides that sensitive personal data can be processed for reasons of public health,[39] such as for the purposes of public health emergencies, including preventing, detecting, and responding to infectious diseases.

---

[32] Part 1 Clause 1.3 (XXV) of the NDPR
[33] Clause 2.6 of the NDPR
[34] Section 65 of the NDPA
[35] Section 30(1)(a) of the NDPA
[36] Section 30(1)(b) of the NDPA
[37] Section 30(1)(c) of the NDPA
[38] Section 30 (1)(g) of the NDPA
[39] Section 30 (1)(h) of the NDPA

A comparison with the General Data Protection Regulation (GDPR) [40] reveals that the grounds for processing sensitive personal data provided under the Act mirror those covered under the GDPR.[41] However, the UK Data Protection Act 2018 provides for an extra level of protection and safeguarding before processing sensitive personal data for some of the grounds provided. [42] For instance, for processing sensitive personal data on grounds of public health, the processing activity must be necessary for the reasons of public interest in the area of public health, the processing of sensitive personal data must also be under the guidance of a healthcare professional, or by any person who in the circumstances, owes a duty of confidentiality under an enactment or rule of law. [43] The Act, however, gives the Commission the power to by regulation or directives, provide safeguards for the processing of specific personal data. [44] It is expected that the Commission will make regulations soon for the necessary safeguards for processing sensitive personal data.

iv. Processing of Children's Personal Data

Under the Act, before processing children's personal data, it is essential to obtain the consent of the parent or legal guardian.[45] Though consent of the parent or legal guardian of a child, that is a person under the age of 18, is required before processing the child's personal data, certain circumstances may require the processing of the personal data of a child without necessarily obtaining the relevant parental or legal guardian consent. These include: When it is necessary to protect the vital interest of a child. When it is carried out for the purposes of education, medical, or social care, and undertaken by a professional owing a duty of confidentiality when it is necessary for legal proceedings involving the child. [46]

Another requirement that may be of particular interest to telehealth organisations is the need for data controllers to implement mechanisms for the purpose of verifying age and consent while using any of the government-approved means of identification.[47] This includes international passports, voter's cards, driver's licenses, etc. Of particular interest to digital health organisations providing telemedicine services and others providing health

---

[40] Article 9(2) of the GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[41] With the exclusion of "Processing of Specific Personal Data which are manifestly made public by the data subject

[42] Section 10(2) of the UK Data Protection Act 2018

[43] Schedule 1, Part 1(3) of the UK Data Protection Act 2018

[44] Section 30(2)(c) of the NDPA

[45] Section 31(1) of the NDPA

[46] See 31 sub (4) (a-c). See also Section 3 excludes certain provisions of the Act from being applicable to data processed in respect of Section 3(2), and the requirement for child consent is among the provisions excluded.

[47] Section 31 (2 and 3) of the NDPA

information services is Section 31 (5) of the Act which provides that the Commission shall make regulations to provide for the processing of the personal data of a child between 13-17+ who specifically requests the provision of electronic services. [48]

V. Cross-border Transfer of Data

The Act prohibits the transfer of personal data by a data controller or processor to a foreign jurisdiction except the recipient is subject to law, corporate binding rules, or certification requirements with equivalent protection.[49] In addition, to this exception, the Act permits other exceptions, including that the data subject has provided consent after being informed of the potential risks of such transfer. This may apply to health data such as personal health information to health facilities abroad. Another exception that is applicable in the health context is where the transfer is for the sole benefit of the data subject and it is not practicable to obtain such consent from the data subject. An example of such a situation may be where a patient is unconscious and his records are to be sent to a facility outside the country.

VI. Sanctions under the Act. (Compliance Orders, Enforcement Orders, Criminal Sanctions)

Finally, healthcare businesses and organisations must understand the various sanctions that may apply to them in the event of non-compliance. The whole process of sanctions starts with a complaint to the Commission, lodged by a data subject (i.e. a patient, or user of a telehealth platform) which the Commission may decide to investigate if the same is not a baseless complaint.[50] The Commission may also decide to initiate an investigation if it feels the Data Controller or Processor which may be a Hospital, Telehealth/telemedicine Platform, or Health Insurance Company, amongst others is in breach of the Act or any of its regulations [51]

Upon carrying out its investigation, if the Commission is of the opinion that there is a breach or there will be a likely breach of any provisions in the Act or any of its regulations. The Commission may issue a compliance order which will offer the data controller, a grace period within which to remedy the breach or prevent the likely breach of the Act or any subsidiary legislation.[52] The compliance order will also provide steps to be taken by the Data Controller/Processor to remedy the breach or prevent the likely breach and also provide for

[48] Section 31(5) of the NDPA
[49] Section 41 (1) of the NDPA
[50] Section 46(1) and (2) of the NDPA
[51] Section 46(3) of the NDPA
[52] Section 47(1) of the NDPA

the right of the Data Controller/Processor to seek a judicial review.[53] The compliance order will come in the form of a warning, cease and desist order, etc. [54] The Data Controller/Processor can decide to align itself with the compliance order or choose to seek redress by applying for a judicial review in a court of competent jurisdiction.[55] The application for judicial review must, however, be done within 30 days of the issuance of the "compliance order"[56]

If the Data Controller or Processor fails to comply with the compliance order within the grace period stipulated in it, or if there is no application for judicial review. The Commission may issue an enforcement order[57] which will come in the form of regulatory sanctions. These regulatory sanctions may be imposed by the Commission either jointly or severally. The Commission, for instance, may decide to order the Data Controller/Processor to pay compensation to the data subject, and also decide to order the defaulter to render accounts for profits made as a result of the breach. The Commission may also decide to impose a fine[58] solely or jointly with any/all other regulatory sanctions such as compensation and accounts for profit.

Notwithstanding, criminal convictions may await defaulters in addition to the regulatory sanctions. [59] The criminal sanctions will only take effect upon conviction. The conviction may be a fine (as already explained in this article) imprisonment of one year or both.

The punishment so imposed by the Court, will not restrict its powers to issue an order of forfeiture against a convicted Data Controller/Processor.[60] The Data Controllers/Processors can also be liable for negligent acts or omissions (which amount to a breach of the Act or any subsidiary legislation of the Act) of third parties for whom they are responsible i.e. employees and agents. [61]

4. Conclusion

The enactment of the Nigeria Data Protection Act is an important milestone for the protection of personal data in Nigeria. As stated earlier, it is important for stakeholders in the healthcare space, being significant data processors, to understand the obligations required under the

---

[53] Section 47(3) of the NDPA
[54] Section 47(2) of the NDPA
[55] The High Court or Federal High Court
[56] Section 50 of the NDPA
[57] Section 48(1) of the NDPA
[58] This has been discussed earlier in the Article
[59] Section 48(1) and 49(1) of the NDPA
[60] Section 52 of the Act
[61] Section 53(1) of the Act

Act. It is expected that other guidelines and regulations will be developed by the Commission which will further set out the obligations of data processors and controllers under the Act. A key matter will be providing clarity on the clause on the processing of data of matured minors between the ages of 13-17+. This will give stakeholders the much-needed guidance to fully comply with the Act. It is important to recognise that privacy and confidentiality provisions as contained in other health legislation continue to subsist, including for instance, the National Health Act. These remain in force. There is a need for healthcare regulators to align all policy documents and practices in line with the NDPA, while at the same time staying informed about regulatory developments.

Authors

Prof Cheluchi Onyemelukwe
Managing Partner

Dotun Bhadmus
Associate

Health Ethics and Law Consulting
Suite 202, Dew International Complex
58 Omorinre Johnson Street, Lekki Phase 1
Lagos, Nigeria
www.healthlaw.com.ng
info@healthlaw.com.ng