STREN & BLAN PARTNERS

CROSS-BORDER DATA TRANSFER IN THE HEALTHCARE SECTOR: LEGAL CONSIDERATIONS AND BEST PRACTICES

www.strenandblan.com

INTRODUCTION

Cross-border data sharing in the healthcare sector is vital for advancing medical research, enhancing patient care, and promoting global health initiatives. It enables stakeholders gain access to a multitude of data, which in turn speeds up medical progress and enhances patient care. However, this practice raises considerable concern, particularly in terms of privacy and compliance with both local and international standards. It involves navigating a complex web of legal considerations and adhering to best practices to ensure compliance with diverse regulatory frameworks, security, and ethical standards.

The legal complexities of cross-border data sharing in healthcare require striking a fine balance between maximizing the benefits of shared data and protecting against potential risks. Key legal considerations include adherence to data protection laws such as the Nigerian Data Protection Act (NDPAct) of 2023, and various national laws that impose stringent requirements on data transfer, consent, and usage. Healthcare data being sensitive data, demands stringent safeguards to ensure confidentiality and integrity.

This article explores the legal considerations and best practices for cross-border data sharing in the healthcare sector.

LEGAL CONSIDERATIONS

1. Data Protection Regulations

Different countries have different data protection laws that control the exchange of personal information. Understanding and adhering to these laws are important to avoid legal issues. Some key international regulations such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States make provisions for data sharing in the healthcare sector, however in this article, we shall be taking a cursory look at provisions of the NDPAct regarding cross border data transfer and its operation in the healthcare sector.

The Act outlines two conditions for cross-border transfers. Firstly, it restricts the transfer of personal data outside Nigeria unless the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, codes of conduct, or certification mechanisms that afford an adequate level of protection with respect to the personal data in accordance with the NDPAct.[1] This is known as the adequacy requirement - as a basis for the cross-border transfer of personal data. Information can be transferred from the healthcare sector in Nigeria to another country if it complies with this provision of the NDPAct or, where there is no adequacy, a data controller or processor may only transfer data if: (a) the data subject consents and does not revoke such consent after being informed of associated risks; (b) transfer is necessary for a contract with the data subject or to take pre-contractual steps at the data subject's request; (c) transfer is for the sole benefit of the data subject and obtaining consent is impracticable; (d) transfer is necessary for important public interests; (e) transfer is necessary for legal claims; or (f) transfer is necessary to protect vital interests of a data subject or others unable to consent.[2]

[1] Section 41(1)(a) of the NDPAct
[2] Section 41(1)(b) of the NDPAct

2. Data Transfer Mechanisms

Pursuant to section 41 of the NDPAct, the first consideration and basis for cross border transfer is the existence of a data transfer mechanism. These mechanisms include: the existence of a data protection law, binding corporate rules, contractual clauses, code of conduct or certification mechanism. These mechanisms provide a legal framework and solution to facilitate data transfers to third party countries.

While contractual clauses are legal contracts that will stipulate data protection requirement for both parties and give a binding commitment to both parties to comply with the principles outlined in the contract, binding corporate rules are internal policies used by multinational corporations to ensure that personal data transferred both internally and across borders conforms with data protection regulations in the countries involved. In order for these mechanisms to be effective, they must be carefully drafted and complied with.

In determining the adequacy of these mechanisms listed in section 41 of the NDPAct, such mechanism shall be assessed taking into account the provisions of section 42(2) of the NDPAct. These assessment measures include:

a. availability of enforceable data subject rights
b. existence if any appropriate instrument between the Nigeria Data Protection Commission (the 'Commission') and a competent authority in the third country that ensures adequate data protection
c. access of a public authority to personal data
d. existence of an effective data protection law
e. existence and functioning of an independent, competent data protection or similar supervisory authority with adequate enforcement power; and
f. international commitments and conventions binding on the relevant country and its membership to multilateral or regional organisations.

It is important to note that in Nigeria, the Commission is required to approve any of such adopted mechanisms before an organisation can rely on them as a basis for their cross-border data transfer. It is also for the Commission to determine whether a country, region or specific sector within a country affords an adequate level of protection under section 42 of the NDPAct. This means that where an organisation within the health sector intends to carry out a cross-border transfer of health data and such organisation is relying on section 41(1)(a) of the NDPAct, then the organisation is required to submit such mechanism to the Commission for approval before carrying out such cross border transfer.

3. Consent

The most primary basis on which data controllers and processors can rely on while processing data is consent. Consent is especially necessary in the health sector where most data processed are the sensitive data of data subjects and these need to be handled with utmost care and secrecy.

As previously stated, in the absence of adequacy of protection, an organsiation may rely on any of the condition in section 43 of the NDPAct, one such conditions being consent.

Consent is a fundamental aspect of cross border data transfer and must be obtained explicitly, with the patients being fully informed and agreeing to the processing and transfer of their personal data. In order to properly obtain consent, there are certain elements that must be involved.

a. Informed Consent: The healthcare facility must provide the patient, in clear, concise and understandable language, information about how the data would be used, who it would be shared with, the countries to which the data would be transferred, the purpose of the data transfer and any potential risk.

b. Voluntary and Unequivocal Consent: The patient must give his/her consent freely without any form of coercion or influence. For example, consent gotten from a patient under the influence of an anesthesia cannot be seen to be voluntary consent. The patients must also be informed of their right to withdraw their consent at anytime in an easy method.

BEST PRACTICES

There are certain best practices that can be adopted by organisations in the health sector to ensure that data transfer across border is done securely and effectively. These practices include:

a. Robust Data Sharing Mechanisms

Implementing robust data transfer mechanism is essential for ensuring compliance with data protection regulations and safeguarding personal data during cross border transfers. Data protection clauses must be included in data sharing agreements. Clear policies and procedures on data handling, protection, and transfer must be developed and maintained within organisations. Data sharing agreements and policies must be tailored to meet local and international requirements of data protection.

b. Implementing Strong Security Measures

Stakeholders in the healthcare sector should implement strong security measures such as data encryption and enable secure channels for data transfer to prevent unauthorized access. Organisations should explore integrating multi-factor authentication to add a layer of security for accessing sensitive data when sharing data across border and leveraging blockchain for secure and transparent cross border data sharing.

It is required that organisations carry out regular security audits and assessments to scan for vulnerabilities in systems handling data transfers.

c. Governance and Accountability

Healthcare facilities are required to designate data protection officers (DPOs) to oversee data protection strategies and ensure compliance with

data protection laws. The DPOs will aid in advising and monitoring compliance as well as acting as a contact person for regulatory bodies relating to processing of data. The DPOs also advise on the necessity for organisations to carry out Data Protection Impact Assessments (DPIAs) to analyse the data processing measures of a new product or service and assess any possible risks to the rights and interest of a data subject by virtue of its nature or purpose.

d. Patient-Centric Approach (Transparency and Trust)

This envisages fostering clear communication with patients about data use and prioritizing the rights and privacy of patients regarding cross border data transfer. Organisations are encouraged to ensure that patients are fully informed about how their data will be used, shared, and protected, enabling them to make informed decisions. By doing this, the healthcare provider will gain the trust of its patients through transparency.

e. Legal and Regulatory Compliance

In order to comply with legal and regulatory requirements, healthcare providers need to understand applicable laws or employ the services of a legal professional that would ensure a thorough understanding of the data protection laws in both the originating and receiving countries as well as keeping them abreast of changes and updates in the regulations to ensure ongoing compliance. In Nigeria, the Commission has licenses professional bodies as Data Protection Compliance Officers (DPCOs) to provide professional data protection compliance services to organisations. It is advisable that healthcare providers and organisations in the health sector in Nigeria engage the services of a DPCO to assist in the organisations ensure compliance in its data processing.

CONCLUSION

Addressing the difficulties of cross-border data transfers in the healthcare sector necessitates a careful balance between legal compliance and operational efficiency. Ensuring compliance with international and local data protection requirements, such as the GDPR and the Nigeria Data Protection Act, is critical to protecting patient privacy and preserving confidence. Legal factors such as gaining express patient consent, adopting strong data security measures, and establishing clear data sharing agreements are all essential components of a compliance cross-border data transfer strategy. By also adopting the previously discussed best practice measures, healthcare providers can reduce legal risks, increase international collaboration, and, ultimately, improve patient care across borders. As the regulatory landscape evolves, remaining knowledgeable and adaptable will be vital to succeed in this constantly evolving sector.

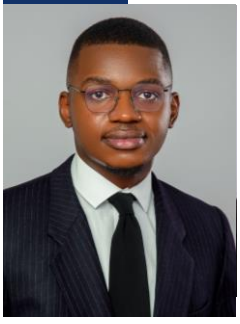
ABOUT STREN & BLAN PARTNERS

Stren & Blan Partners is a full-service commercial Law Firm that provides legal services to diverse local and multinational corporations. We have developed a clear vision for anticipating our clients' business needs and surpassing their expectations, and we do this with an uncompromising commitment to Client service and legal excellence.

THE AUTHORS

Amala Umeike
Partner

Amalaumeike
@strenandblan.com



Emmanuel Ughanze
Associate

Emmanuelugghanze
@strenandblan.com

Justina Okachi
Associate

Justinaokachi@strenandblan.com

Stren & Blan Partners

+234 (0)702 558 0053
3 Theophilus Orji Street, Off Fola Osibo Road, Lekki Phase 1, Lagos, Nigeria

www.strenandblan.com
contact@strenandblan.com
@strenandblan