Cloud & Third-Party Compliance Statement

Effective Date: 20/03/2025
Last Updated: 20/03/2025

1. Introduction
Flyte Technologies and Solutions Ltd provides software solutions to healthcare organizations. While we do not process or store patient data, our clients may deploy our software on third-party cloud services. This statement clarifies compliance responsibilities related to cloud and third-party services under the Nigeria Data Protection Regulation (NDPR).

2. Scope
This document applies to clients who deploy our software on external cloud providers (e.g., AWS, Microsoft Azure, Google Cloud, Digital Ocean) or integrate it with third-party services.

3. Responsibilities of the Client (Data Controller)
Since our company does not host or manage client data, clients are responsible for:

- **Ensuring NDPR compliance** when choosing cloud providers.
- **Configuring security settings** to protect patient data.
- **Conducting due diligence** on third-party service providers.
- **Managing access controls** within their cloud environment.

4. Our Responsibilities (Software Provider)
We ensure:

- Our software supports **secure deployment on cloud services**.
- **Encryption and access control mechanisms** are built into our software.
- We provide **guidance on secure implementation** of our software.
- We offer **updates and patches** to mitigate security vulnerabilities.

5. Cloud Provider Compliance
Clients should verify that their chosen cloud provider:

- Complies with NDPR and international data protection standards (e.g., ISO 27001, GDPR).
- Provides adequate data security, encryption, and access control mechanisms.
- Has appropriate **Data Processing Agreements (DPA)** in place.

6. Data Breach and Incident Response

- The Client is responsible for **monitoring and reporting data breaches** in their cloud environment.
- We provide **security patches** and updates to help prevent vulnerabilities.
- Clients should establish **incident response plans** with their cloud providers.

7. Limitation of Liability
As we do not host or process patient data, we are **not liable for security incidents** occurring in third-party cloud services. Clients assume full responsibility for their chosen deployment environment.

8. Contact Information
For questions regarding cloud security and compliance, contact: connect@ftsl-ng.com

---