RFK HOSPITAL
COMPASSION, INNOVATION, CARE.

RFK HOSPITAL SECURITY OBJECTIVES

1. DOCUMENT DETAILS

VERSION:	VERSION 1.0
DOCUMENT OWNER:	IT SECURITY & COMPLIANCE TEAM
PREPARED BY:	ADEYINKA OGUNDELE
APPROVAL DATE:	APRIL 01, 2025.
APPROVED BY:	CTO - MR. REGBE SCOFIELD
REVIEW CYCLE:	ANNUALLY
CLASSIFICATION:	INTERNAL (RESTRICTED)

1.1 Introduction

Rẹ̀mí-Fíbíke-Kọ́lá Specialist Hospital (RFK Hospital) is a globally-focused healthcare provider, dedicated to excellence in patient care, medical research, and technological advancement. With our home office in Lagos, Nigeria, we remain committed to maintaining the highest standard of healthcare security, ensuring robust cybersecurity, data protection, and regulatory compliance, to safeguard all our hospital operations, and maintain trust in the services we offer.

This document outlines core RFK's security objectives that guide our cybersecurity, risk management, and compliance strategies to ensure the confidentiality, integrity, and availability of our systems and data.

1.2 Mission and Vision

At RFK Hospital, our vision is to lead the healthcare industry by delivering innovative and affordable technological solutions to patient care by the year 2040.

Our Mission: With a foundation built on *Compassion, Innovation, and Care*, we are committed to world-class healthcare while upholding the highest standards of data security, patient privacy, and regulatory compliance.

2. PURPOSE & SCOPE

The information in this document defines the security objectives for RFK Hospital. It applies to all our employees, medical staff, third-party vendors, and stakeholders handling patient and hospital information. The objective covers the following critical areas:

- Electronic Health Records (EHR) Systems
- Patient Data - Personal Health Information(PHI) ,and Personal Identifiable Information (PII)
- Medical IoT Devices & Healthcare Systems
- Hospital IT Infrastructure
- Third-party & Vendor Risk Management
- Staff & Employee Access Control
- Physical Security & Facility Access
- Cloud & Remote Access Security

This ensures Confidentiality, Integrity, and Availability across all hospital operations.

3. DATA CLASSIFICATION

At RFK Hospital, data is classified based on sensitivity and impact to ensure appropriate protection measures. Specific classifications, handling procedures, and access controls are detailed in the Data Classification Policy.

4. SECURITY OBJECTIVES

At RFK Hospital, our security objectives establish a strong foundation for safeguarding patient data, hospital operations, and information assets. These objectives align with global and local regulatory requirements, ensuring the confidentiality, integrity, and availability (CIA) of all data.

4.1 Confidentiality

- Protect patient data, including Personally Identifiable Information (PII) and Protected Health Information (PHI), from unauthorized access or disclosure.

- Implement strict access controls to ensure that only authorized personnel have access to sensitive data. This includes multi-factor authentication (MFA) for accessing critical systems.

- Secure communication channels for data transmission, both internally and externally, using encryption protocols.

- Ensure compliance with NDPR, ISO 27001, HIPAA, and other relevant standards, such as conducting periodic audits to assess compliance.

4.2 Integrity

- Maintain the accuracy and reliability of patient records and medical data by implementing data validation mechanisms.
- Implement measures to prevent unauthorized modification of critical information, including role-based access controls and data encryption at rest.
- Establish audit trails and logging mechanisms to track data changes and ensure accountability, enabling detailed review and traceability.

4.3 Availability

- Ensure critical healthcare systems remain operational and accessible when needed by implementing high availability solutions and redundant systems.
- Implement robust disaster recovery and business continuity plans, including regular testing to ensure minimal downtime in case of disruption.
- Protect IT infrastructure from disruptions caused by cyber threats, system failures, or natural disasters by using advanced monitoring tools and vulnerability management programs.

4.4 Risk Management

- Identify, assess, and mitigate risks associated with patient data and hospital operations through regular risk assessments, conducted annually and whenever significant changes occur.
- Perform continuous monitoring using automated tools to detect emerging threats and vulnerabilities.
- Implement tailored risk mitigation strategies, including regular security assessments, vulnerability scanning, and penetration testing, to proactively address security gaps.
- Engage in ongoing cybersecurity training for staff to enhance their understanding of risk factors and their role in mitigating them.

4.5 Compliance & Regulatory Adherence

- Align security policies with applicable healthcare security and privacy regulations, including NDPR, HIPAA, and ISO 27001.
- Ensure adherence to these standards through regular audits, internal reviews, and documented evidence of compliance efforts.
- Establish continuous improvement mechanisms to stay updated with evolving regulations, ensuring that RFK Hospital maintains a high level of regulatory compliance at all times.

4.5.1 Regulatory Frameworks

RFK Hospital operates under the following regulatory frameworks to ensure compliance and data protection:

- **HIPAA (Health Insurance Portability and Accountability Act):** U.S. regulation for protecting patient health information (PHI).
- **ISO 27001:** International standard for information security management systems (ISMS), which provides a framework for managing sensitive company information.
- **NIST Cybersecurity Framework (CSF):** Provides guidelines for identifying, protecting, detecting, responding, and recovering from cyber threats.
- **NDPR (Nigeria Data Protection Regulation):** Nigeria's data protection regulation ensures privacy rights and the security of personal data.
- **GDPR (General Data Protection Regulation)**: As RFK Hospital may treat EU nationals, we ensure compliance with GDPR, which regulates the privacy and security of personal data for EU citizens.

4.6 Security Awareness & Training

- Educate our staff on cybersecurity best practices and data protection policies through ongoing training programs, conducted quarterly, to ensure staff are consistently updated on the latest security practices.
- Conduct regular training sessions to reduce human-related security risks, including phishing awareness, password management, and handling of sensitive data.

- Foster a security-conscious culture within the organization by promoting awareness campaigns and incentivizing staff for compliance.

4.7 Third-Party & Vendor Security

- Establish robust security requirements for third-party vendors handling RFK Hospital data, ensuring they comply with RFK's security policies and regulations.
- Mandate third-party vendors to undergo security assessments (e.g., penetration testing, security audits) to ensure they meet RFK's security standards.
- Include data protection and security clauses in vendor contracts to hold third parties accountable for compliance.
- Perform regular security assessments on external partners to ensure continued adherence to RFK's security objectives and policies.

4.8 Physical Security & Facility Access

- Implement strict physical access controls to prevent unauthorized access to hospital facilities and sensitive areas, including biometric access systems and security personnel.
- Ensure that physical security measures, such as video surveillance, perimeter security, and access logs, align with RFK Hospital's overall security objectives.
- Protect critical infrastructure from physical threats, such as theft, vandalism, or natural disasters, by using environmental controls and physical barriers.

4.9 Incident Response & Recovery

- Develop and maintain an incident response plan (IRP) to quickly address and mitigate security breaches and cyber threats. This plan includes predefined escalation paths, containment strategies, and designated roles for incident response team members.
- Conduct regular tabletop exercises and live simulations (at least annually) to test the effectiveness of the incident response plan and ensure staff familiarity with emergency protocols.
- Ensure rapid response and recovery from security incidents by maintaining an incident response team (IRT) with specialized skills, clear roles, and access to the necessary resources.

- After each incident, perform a post-incident analysis to identify root causes, assess the impacts, and implement improvements to strengthen security measures, reducing the likelihood of similar incidents occurring in the future.

5. REVIEWS AND UPDATES

This document will undergo a comprehensive review at least annually or sooner if there are significant changes in:

- Relevant regulations and industry standards.
- Hospital operations, systems, or infrastructure.
- Identified cybersecurity risks or emerging threats.

Any necessary updates will be reviewed and approved by RFK Hospital's IT Security & Compliance Team, ensuring that the security policies remain aligned with both the hospital’s operational needs and evolving regulatory requirements.