SERVICE ORIENTED ARCHITECTURE

POLICY FOR A CARE COMPANY

QMB

CRECIX CARE LIMITED

1. Purpose and Introduction

This policy outlines a structured, secure, and compliant Service -Oriented Architecture framework to guide the development, deployment, and management of IT services at Crecix Care Limited. The purpose is to enhance the quality of patient care through secure data integration, interoperability, and scalability of the healthcare system.

By implementing service-oriented architecture, Crecix Care Limited enables seamless data across various systems such as electronic health records (EHR), telehealth services, patient monitoring platform ensuring real-time patient- centred care delivery.

2. Scope

This policy applies to all technology platforms, applications, and services used for healthcare delivery at Crecix Care Limited. This governs all employees, contractors, vendors, and third-party service providers involved in design, implementation or maintenance of SOA based systems including but not limited to electronic health records systems, patient and care management platforms, telehealth services, data-sharing interfaces with external healthcare providers and health monitoring systems.

3. Roles and Responsibilities

- ***SOA Steering Committee:*** Responsible for overseeing the SOA strategy and ensuring that it aligns with the organization operational and clinical goals. The committee will also review major changes and updates to the SOA framework.
- ***Healthcare IT Architect:*** Leads the design and technical implementation of services, ensuring compliance with the SOA framework and addressing any technical challenges in service integration.
- ***Compliance and Security Officer***: Monitors compliance with healthcare regulations, conducts regular audits and ensure that data security practices meet HIPPA, GDPR and relevant laws.
- ***Clinical and Operational Leaders:*** Provide input on how services should integrate with clinical workflows, ensuring SOA supports the practical needs of care providers.
- ***Security Teams***: Oversees security controls, monitoring for potential threats, vulnerabilities, and handling security incidents.
- ***Developers and IT Teams***: Responsible for implementing services according to the SOA design, controls and ensuring proper integration with existing systems.

4. Principles

To ensure consistency, security, and quality the following principles will serve as a guide for the SOA design and implementation at Crecix Care Limited.

- All services must prioritise the patient's needs ensuring prompt and secure access to critical information, improving care coordination and minimising data silos.

- Services (patient record retrieval, appointment scheduling) should be designed to work across different systems without the need for major rewrites. This ensures a more cost-effective and time-efficient deployment across multiple care centres.
- Systems and services must adhere to healthcare interoperability standards such as HL7, FHIR, and DICOM to ensure data exchange between internal systems and external healthcare partners. Compliance and regulations like HIPAA and GDPR must be maintained at all times to protect patient data.
- All services must comply with HIPAA and GDPR to safeguard patient data. This includes encryption of sensitive information, access controls, and audit logs. Data breach reporting mechanisms must also be established to ensure swift response in the event of unauthorized access.
- Services must be scalable to accommodate an increasing number of patients, devices, and data points. As Crecix Care Limited grows or integrates with other healthcare systems, the architecture should allow for seamless expansion and integration.
- Each service should function independently of other systems, minimizing dependency. This allows upgrades, repairs, or replacements to occur without disrupting other services.
- All services must be continuously monitored for performance, compliance and security. Real time monitoring tools should be used to detect issues and prompt timely interventions. Services should be regularly updated to remain in line with evolving healthcare standards.

5. Controls Framework

The following controls are implemented to ensure that the SOA framework remain secure, compliant, and aligned with Crecix Care Limited operational objectives:

- All patient's data must be encrypted during transmission and at rest. Encryption algorithms should meet industry standards.

- Only authorised personnel will have access to specific services and patient data based on their roles. Sensitive operations will require multi-factor authentication.
- All access to patient data and sensitive services must be logged. Audit logs should be protected against tampering and reviewed regularly for any suspicious activity.
- All services must be compliant with healthcare regulations, including GDPR. Service should only access and process the minimum data necessary to perform their functions.
- Third party services or vendors interacting with patient data must adhere to the same security and compliance standards as internal systems. Regular security assessments and vendor audits should be conducted.
- Regular security audits must be conducted for all services with a focus on system handling sensitive data. Vulnerabilities must be addressed immediately.
- Real time monitoring must be implemented for all critical services to ensure high availability and detect performance issues early. Automated alerts should be set up for service failures, slowdowns, or unusual activity.
- A formal change management process must be followed for all service updates. This includes testing in a sandbox environment, a risk assessment and ensuring that changes do not disrupt clinical workflows or patient data access.
- A clear incident response plan must be in place to handle any service disruptions or security breaches. The plan must define roles, timelines for response and reporting mechanisms to stakeholders and regulatory bodies.
- All service must follow a defined lifecycle that includes design, testing, deployment, and maintenance. Each stage must include a security and compliance review to ensure the service meets SOA standards and healthcare regulations.

6. Framework Components

The following architectural components from the foundation of Crecix Care Limited-Service Oriented architecture.

- A central repository of all services, their descriptions and interfaces allowing for easy discovery and reuse of services across the organisation. The registry should be updated as services are added or modified.
- A secure gateway for managing service access and external data integration ensuring that only authenticated and authorised entities interact with internal services. The gateway must enforce rate-limiting, security policies and traffic monitoring.
- The central layer responsible for managing the consistency, accuracy, and availability of patient data across various services. The data management layer must ensure data integrity and support failover mechanisms to prevent data loss during service outages.
- A communication hub that orchestrates data exchange between services, ensuring that messages are routed appropriately and transformed where necessary to ensure interoperability between systems.

7. Review and Compliance

This policy is reviewed annually in response to changes in technology, healthcare regulations and organisational needs. Failure to adhere to this policy may result in disciplinary actions including termination for employees and contractual penalties for vendors.

References

- U.S. Department of Health & Human Services, https://www.hhs.gov
- Official EU GDPR Portal, https://gdpr-info.eu
- HL7 and FHIR: https://www.h17.org/fhir/
- NIST Cybersecurity Framework: www.nist.gov