KYTHERA™
DECIPHERING HEALTHCARE

Security & Compliance Posture

Overview

Kythera is committed to maintaining a robust security and compliance framework to protect customer data, intellectual property, and business operations. Our security program aligns with industry best practices, regulatory standards, and a risk-based approach to mitigate cyber threats effectively. Additionally our compliance program is structured to align with the OIG's Seven Elements of an Effective Compliance Program, ensuring that we uphold the highest ethical and regulatory standards.

Security Governance & Compliance

- **Dedicated Security Team:** Oversees security controls, monitoring, incident response, business continuity and disaster recovery.
- **Risk and Compliance Team**: Manages the organization's risk framework, policy enforcement and training.
- **Executive Oversight:** Regular security and compliance reporting to leadership ensures ongoing improvements and feedback loop.
- **Continuous Monitoring**: Periodic security assessments and audits ensure a solid security posture and compliance.

Kythera adheres to industry-recognized security and privacy frameworks including:

NIST 800-53- Security controls and risk management best practices
NIST CSF- Cybersecurity Framework
ISO 27001- Information security management system
SOC2 Type II- Secure handling of customer data
HIPAA Compliance- Safeguarding protected health information
And **CMS ARS** control framework

Security Policies and Controls

- **Access and Identity Management**: Multi-factor Authentication for Network and Production Access, Role- Based Access (RBAC) with least privilege access enforcement, all privileged user audit logs regularly reviewed.
- **Data Protection & Encryption:** Encryption in Transit & At Rest: AES-256 for stored data, TLS 1.2+ for data transmission. Data Loss Prevention (DLP) prevents unauthorized data access and exfiltration.
- **Endpoint and Network Security:** Bring your own device (BYOD) Security enforced Mobile Device Management (MDM) and Endpoint Detection and Response (EDR). Cloud security posture with cloud security monitoring.
- **Threat Detection & Incident Response:** 24/7 Security Operations Center (SOC), Incident Response Plan (IRP) is regularly tested via Tabletop Exercises with various scenarios.

Privacy & Data Protection

- **Privacy Policies & Compliance:** HIPAA, Data Retention & Deletion policies ensure timely data disposal. Data Classification and Handling policies ensure privacy and confidentiality requirements for data throughout the entire information lifecycle.
- **Automated Data Processing:** HIPAA-compliant de-identification, tokenization and cleansing are core Kythera capabilities performed before data is transferred into our Wayfinder environment.

Risk Management & Business Continuity

- **Risk assessment and cloud security testing:** monthly risk evaluations, continuous cloud vulnerability scanning and patch management, third party vendor evaluations.
- **No offshore:** data is not stored nor accessible from outside the United States. All Kythera support, services and resources are based in the US.
- **RTO/RPO objectives**: inherited from AWS (99% uptime).

Customer Security Engagement

- **Security Assessment:** assistance during procurement.
- **Dedicated Security and Compliance team:** available for customer inquiries.
- **SLA's:** ensure data availability of 99.9% and response times within 4 hours for critical issues.

This document offers a high-level summary of Kythera's security, compliance, and privacy commitments. All Kythera systems operate in cloud-based environments, specifically AWS and Databricks, allowing Kythera to benefit from a wide range of inherited security certifications and protections.

Kythera is SOC 2 Type II certified.