RISK AND COMPLIANCE

Introduction

As a Software-as-a-Service (SaaS) vendor, Kareo offers independent healthcare practices a secure platform to manage their services and sensitive documentation, including electronic-protected health information (ePHI) data. Changes to the medical field are not only impacting the way doctors practice medicine, but also requiring providers to do more to protect patient data. Kareo is dedicated to helping doctors build an industry-leading security program to ensure all patient data is safe and protected.

Security at Kareo

Kareo's commitment to security includes housing all services on a highly secure and controlled platform in our Kareo cloud data center. To ensure a top level of security, Kareo implements the best practice security frameworks, using both in-house and third-party tools and services. The company also keeps current on industry certifications and independent third-party attestations, or verifications, which are described in this document. This document was created to assist customers in understanding the security controls in place and how those controls have been validated.

Third-party Security Audits

Third-party attestations and certifications of Kareo provide a high level of validation of the control environment. By knowing their data is secure, customers can focus more on their practices and patients. Since Kareo is subject to various internal and external risk assessments, Kareo's compliance and security teams have established an information security framework and policies based on:

- Health Information Trust Alliance (HITRUST) framework**
- AICPA Trust Criteria Security, Confidentiality and Availability
- National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems)

***HITRUST is a United States organization that has established a common security framework (CSF) that can be used by all organizations that create, access, store, or exchange sensitive and/or regulated data.*

External Threat Assessments

The Kareo Security team regularly scans all Kareo services for vulnerabilities and notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to Kareo leadership and are prioritized for remediation. It is important to note that these scans cover the Kareo services and are not meant to replace any validations by its customers required to meet their specific compliance requirements.

Administrative Safeguards

Kareo manages a comprehensive set of policies, processes, and control activities that leverage various aspects of Kareo's overall security program. Kareo has integrated applicable general and cloud-specific security practices identified by leading cloud computing industries and healthcare bodies into the Kareo security program. Kareo continues to monitor these groups for practices that can be implemented to better protect ePHI and PHI data.

Data Protection from the Top down

Security at Kareo begins at the highest level of the company. Executive and senior leadership play important roles in establishing the company's tone and core values. Every employee is provided with the company's Code of Business Conduct and Ethics document and completes training upon hiring and on an annual basis thereafter. Developers receive additional training on security practices and tools. Ongoing compliance audits are performed so that employees understand and follow established policies.

Data Handling

Kareo has strict (e)PHI, PCI, and PII handling requirements, which includes tamper-proof disposal systems and processes. Examples include badge-based printing to eliminate the possibility of loose hardcopy documents for unauthorized access or data loss. Using centralized, role-based access permissions helps ensure that access is only provided to specific personnel who need access to perform essential business functions.

Data Encryption

Kareo encrypts sensitive data using military-grade encryption. When sensitive files are sent to Kareo, they are encrypted over the Internet and encrypted again when they are stored in Kareo's systems. This extra step is taken to minimize the possibility of data loss and unauthorized access.

Secure Networking

Kareo utilizes world class, top tier data centers, firewalls in all data-center and corporate offices, and TLS and application firewalls. Moreover, to ensure Kareo's network remains secure, the company has 24/7 security monitoring combined with industry-leading 3rd-party threat monitoring, assessment, and protection services.

Incident Management

Kareo takes the job of protecting your ePHI data seriously. As part of our security commitment, Kareo has implemented a formal Incident Management Program, which follows the guidelines of local and federal laws for reporting and investigating requirements in accordance with HIPAA rulings.

Kareo Certifications and Third-Party Attestations

Kareo engages external certifying bodies and independent auditors to ensure the policies, processes, and controls established and operated by Kareo meet or exceed applicable regulatory requirements and industry best-practices.

Kareo enables covered entities, which includes their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA), to leverage the secure Kareo work environment to process, maintain, and store protected health information. Kareo signs business agreements with these such customers.

The HITRUST CSF is a security framework that incorporates and leverages many existing security requirements organizations must comply with. This includes federal requirements such as HIPAA, state requirements such as Massachusetts 201 CMR 17.00 and Texas Health and Safety Code 181, and third-party requirements such as PCI and COBIT. It also includes other governmental agencies such as NIST, FTC, and CMS.

Kareo has obtained a service auditor's examination report, which includes an opinion on the suitability of the design and operating effectiveness of the controls based on the American Institute of Certified Public Accountants' (AICPA) Trust Services Principles and Criteria (TPA Section 100). These controls are related to security, availability, and confidentiality.

Kareo regularly performs self-assessments of the PCI DSS under the Payment Card Industry (PCI) Data Security Standard (DSS) for the handling of credit card information.

Penetration Testing

Kareo uses class leading penetration testing services from Veracode. Veracode's manual security testing processes leverage highly specialized tools, custom testing set-ups, and shrewd hacking techniques to identify and mitigate website security vulnerabilities.

Kareo Cyber Liability Coverage

Security is important to Kareo and to further protect our customers, Kareo owns industry-leading cyber liability insurance. Kareo's liability insurance covers the following claims:

- Business Interruption and Data Recover Services
- Crisis Management and Computer System Extortion
- Credit Monitoring Services
- Forensic and Legal
- Public Relations Services

Frequently Asked Questions

How reliable are Kareo's services?

Kareo guarantees an annual uptime SLA of 99.9% with a historical 99.95% uptime. Kareo also manages a disaster recovery location to ensure continued service during the most catastrophic events.

How often is my data backed up and for how long?

Kareo backs up data bases every two hours and will keep them for 30 days. The backups are then transferred to separate Kareo-owned data centers to further protect your data.

What are Kareo's data retention and ownership policies?

Your data remains with you. Kareo will never sell or share your data with a third party. Upon request, Kareo will send all patient data to the customer and remove it from Kareo's systems at time of service cancellation.

Where does my data reside?

Kareo stores all ePHI data in two top-tier 3rd party data centers in the US.