Security Notice

How We Protect Your Data on Our Web-based Software Services

What This Security Notice Covers

This security notice pertains to the security measures in place at Kareo for protection of personal and protected health information in connection with the use of the Kareo web site, and the Kareo Billing (PM), Kareo Clinical (EHR), Kareo Analytics and Kareo Engage web-based services (collectively, Service).

Unique identification of users

To comply with the HIPAA requirements and to provide a secure service, Kareo requires all users to have a unique username. Kareo currently requires a valid email address to be the username for the Kareo Service.

In addition to a username, every user account must be protected with a password of sufficient complexity. Kareo allows its customers to set their own password complexity policy. If your user account has access to multiple Kareo customers, you will be required to use the more restrictive policy.

All Kareo Service sign-ins are protected by account lock-out systems. If a user incorrectly authenticates a number of times or the user's account is locked by a system administrator, their user account will be locked until a system administrator of the user 's account unlocks it. Kareo's support team is prohibited from unlocking user accounts unless the account is the system administrator account.

Security on the Kareo web site

Kareo Service users may choose to sign into their account at the Kareo web site in order to access the downloads or account status. Such sign-ins are protected by SSL security. Your browser will usually display an indicator (such as a "lock" icon) when using a secure SSL connection.

Security in the Kareo service

The Kareo Service communicates with secure Kareo hosted and controlled servers and networks. All communications are secured with public-key encryption. Kareo disallows the use of low cipher strength in our production service.

Kareo helps to ensure physical and technical security protections of customer data, as it uses servers located in SOC 2 type 2 certified hosting providers.

Kareo employs redundant, next-generation firewalls, intrusion detection and prevention services monitored 24X7X365. Kareo uses a PCI Approved Scanning Vendor (ASV), internal and external threat prevention delivering timely and accurate reports of our production services.

In addition to these controls Kareo deploys up to date advanced threat protection services which help to identify, block, and track hacking attempts, scans, data breaches, adware, malware, spyware, Trojans, phishing attempts and other equally malicious requests.

Role-based security

Every user in the Kareo Service belongs to one or more roles. A role is defined by each customer, and is assigned a set of permissions. Kareo roles follow an allow-then-deny pattern of applying permissions — such that multiple role permissions are combined, and then filtered against any role's restrictions.

Application locking

In accordance with HIPAA policies, Kareo's Service will automatically lock up if left unattended for a period of time. Correct credentials of the user will need to be provided prior to using the application again.

Kareo password policy

Kareo system passwords are meant to help protect sensitive patient medical and financial records, as well as practice financial information. They serve as a deterrent to malicious agents as well as protection against casual or accidental lowering of security through carelessness.

The passwords are encouraged to be at least (8) eight characters long and have to maintain a level of complexity such that they will not be easily guessed or cracked by a determined attacker.

A user may change their password at any point in the application or the Kareo web site. Passwords changed by third-parties will immediately expire to allow users to log in but also to ensure that they immediately change their passwords to something that only they know.

Kareo will never store any passwords in permanent storage in a way that is reversible. The Kareo Service will never show the password in plain-text, human-readable form.

Changes to this security policy

Kareo may update this policy at any time for any reason. If there are any significant changes to how we handle security we will make a reasonable commercial effort to send a notice to the contact email address specified in your company's Kareo account or by placing a prominent notice on our site.

Questions?

If you have questions or suggestions you can contact us at:

Kareo Security Administrator
1111 Bayside Drive Suite 150
Corona Del Mar, CA 92625
security@kareo.com

To report a security violation, please call us at 888-77-KAREO (888-775-2736).

Last Updated: This policy was last updated on June 19, 2019
For terms effective for purchases prior to June 19, 2019, click here.