Tricefy Safety & Security

Last Modified on 03/25/2022 7:53 am EDT

How we protect your data

The security of our client's data is our highest priority. The Tricefy cloud service is designed with multiple layers of state of the art security across a scalable, secure infrastructure. We enforce policies and process controls to safeguard access to information and use third-party auditors to ensure that we remain compliant.

Datacenter Security

Tricefy is hosted by Amazon Web Services (AWS), which is the market leader in infrastructure security. AWS is one of very few providers that is C5 compliant and equipped to handle medical data. This makes them uniquely qualified to provide the most up-to-date and safest environment for handling sensitive and important data.

The AWS servers used by Tricefy do not have Windows components nor access points, which eliminates the threat from malware so common today.

Secure Data Transfer – Tricefy Uplink

Tricefy Uplink transfers data through a sophisticated, one-directional, impenetrable tunnel from your client's network to the Tricefy servers. Data is transferred using a secured internet connection with industry best-practice encryption and transmission (TCP/TLS PSK). All data is encrypted in an unreadable format that is only consumable to those with the correct key (a cryptographic identity).

During transit (as data is sent to Tricefy), data is encrypted using Transport Layer Security (TLS 1.2), which creates force field around our tunnel. Once the data arrives safely to our servers, it is encrypted using AES256 file storage encryption.

This is the same level of security trusted by top government and financial institutions.

Access Control

Tricefy allows very long and complex passwords. Additional security is implemented using multi-factor authentication in the form of OATH-OTP, which is a one-time verification code used by many companies, including Google.

Compliance

Compliancy is an effective way to validate trustworthiness of a service. We encourage and expect our customers to verify that our security practices comply with the most widely accepted standards and regulations, including (but not limited to):

- ISO 13485
- General Data Privacy Regulation (GDPR)
- U.S. Food and Drug Administration (Class I medical device)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- SOR98-282 Canadian Medical Device Regulations
- India's Information Technology Act 2011
- Singapore Data Protection Act, 2012
- Turkish Personal Data Protection Law, 2016

Now you see why large healthcare organisations and private clinics in more than 43 countries reviewed our security concept and trust us with their data. They use Tricefy every day to securely archive and share their medical data.

For more information about Tricefy safety and security, please see the following Tricefy Help Center articles:

Trice Imaging Information Security Policy