Security and privacy of your data is paramount to us.

Here you can learn about how we safeguard it.

Application security

Protecting your therapyBOSS account

Two-factor authentication

Required for web access from unrecognized devices. Remembered for 30 days if browser cookies are enabled.

Permission-based access

Office staff accounts are permission restricted. Clinicians only have access through their own interfaces and only to assigned patients.

User management

One place to add and manage office staff. Last login timestamp to monitor activity. Lockout for failed login attempts. Related email notifications.

User data security

Protecting your data in therapyBOSS

Data encryption

All data communication is encrypted with TLS 1.2. For data in storage,

Mobile app encryption

Mobile app stores data on devices to be able to work offline. This data is

Encoded passwords

Account passwords are hashed in the database to be indecipherable.

AES 256 bit encryption is employed.

secured with AES 256 bit encryption.

Forgotten passwords must be reset.

Data center security

Protecting our networks and infrastructure

Virtual Private Cloud

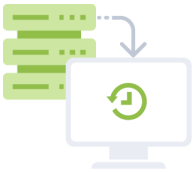
Hosted in a dedicated private cloud. Firewall rules and software defined networking with all connections encrypted.

World-class hosting

Local (Chicago area) data center. SSAE18 Type 2, SOC1, SOC2 compliance. 24/7 physical security and protection.

Access controls

Access into production networks is restricted by IP address and possible only by a few authorized members of our team.



Disaster recovery

Ensuring business continuity

Redundancy

Every component of our network infrastructure is essentially duplicated to deliver resiliency in the face of system failures.

Data backup

Comprehensive backup strategy ensures that all data is backed up frequently and backups are ready for restoration.

Stand-by data center

Real-time data replication to a geographically separated hosting environment for seamless continuity.

Credit card security

We don't store credit cards. Further, our applications are intentionally designed such that sensitive information you enter when adding or editing your payment method is not accessible to us. Our credit card processing vendor uses security measures to protect your information both during the transaction and after it's complete. Our vendor is certified as compliant with card association security initiatives including the Visa Cardholder Information Security and Compliance (CISP), MasterCard® Site Data Protection Program (SDP), and Discovery Information Security and Compliance (DISC).

Your responsibilities

Keeping your data secure also requires that you do your part by using a sufficiently complex password, storing it safely and not sharing it with anyone. Change your password and answers to security questions immediately if you suspect that your login may have been compromised. Terminated staff should have their logins disabled. You should also ensure that you have adequate security on your own systems and networks.

Responsible disclosure

If you have found any potential vulnerability in the therapyBOSS application, please act responsibly by not sharing it publically. Report the issue by calling us at 847-581-6400, emailing security@pragmait.com or clicking the button below. Our team will acknowledge your inquiry within 48 hours. We investigate all reported security issues to assess their impact and take commensurate measures to address them.

If you believe your therapyBOSS account has been compromised, please reset your login immediately. If you require assistance, contact technical support by calling at 847-581-6400 or emailing support@therapyboss.com.