Bloominmind Security Policy

Last updated: October 09, 2020

Bloominmind HealthTech Inc. acts as a trusted confidential application service provider dedicated to providing a secure Internet and mobile service.

Bloominmind HealthTech employs a high degree of security consciousness. One of Bloominmind's priorities is to make reasonable efforts to ensure data security and be fully compliant with all HIPAA regulations. Access, integrity, availability, ownership, authorization, dependability, authentication, and confidentiality are all major considerations within the Bloominmind Security Policy. Unfortunately, the Internet cannot be guaranteed to be 100% secure, and we cannot ensure or warrant the security of any information you provide to us.

Bloominmind upholds its stringent Security Policy with the following security measures:

1. Role-Based Usage

Bloominmind grants varying degrees of access to users with different levels of authority within a provider practice.

2. Encryption

All communication between you and the Bloominmind server is secured by using SSL AES 256-bit encryption. This is the highest level of encryption currently available commercially.

3. Data Security

Bloominmind takes measures to secure your data on our servers, in our data center. Our data center is both physically and electronically secured. Our servers are isolated from the Internet by using a firewall which is a hardware and software system that blocks access by unauthorized parties.

4. Confidentiality

Bloominmind has internal policies that keep your data private and confidential. We will not share your data with any third party except as described in our Privacy Policy. Your data is your data only.

5. Login ID and Password

Access to your account is controlled by a login ID and a password, which you chose. Strict login ID and password rules help prevent unauthorized users from gaining access to data. We do NOT store a plain text version of your password. Your password is stored using a one-way hash key and verified using the same one-way hash every time you login, which means no one at Bloominmind knows what password you have chosen. If you ever forget your password, we force you to choose a new one using an email verification check.

6. Auto Log Out

Bloominmind protects you against accidentally leaving your account active on a computer browser screen. The Bloominmind service ends your "session" if you are logged into Bloominmind but have not actively used the service for a set period of time. This prevents others from accessing your account when you leave a session and forget to log out.

7. Sensitive Information

Bloominmind handles all your health information with respect to its confidentiality and privacy. We ask that you follow your provider's policy on communicating sensitive information in their practice.

8. Data Integrity

Bloominmind employs products and technology to help ensure data is available and access to the site continues without interruption.

9. Storage and Maintenance of Information

For more information regarding the storage and maintenance of information,
please contact Bloominmind support.

10. Firewall

We take reasonable measures to secure your data on our servers, in our data center. Our data center is both physically and electronically secured. Our servers are protected behind the Internet by using a firewall system that blocks access by unauthorized parties.

11. What can I do to protect my Privacy?

To protect your privacy while using Bloominmind, you can:

- Never share your sign in name or password.
- Always sign out when you are finished using the service.
- Choose a strong password that consists of upper- and lower-case letters and numbers.
- Install and maintain anti-virus software and a firewall on all computers that you use to access the Bloominmind service.
- Promptly install all security and software updates for our iPad/iPhone apps, your web browser, and computer operating systems.