pickAtime Data Security and Privacy

Security and Privacy on the pickAtime website is very important to us.

Data Security

Our site has security measures in place to help protect against the loss, misuse, and alteration of the data under our control. We use Secure Socket Layer (SSL) technology to encrypt all data transmissions between your browser and our servers. SSL technology uses both server authentication and data encryption to ensure that your data is safe, secure, and available only to authorized users in your organization. A dedicated and robust firewall provides a strong barrier of network security from the Internet. Additionally, we employ AES-256 encryption for data at rest.

Access to client accounts requires a login with a unique username and password. These passwords can be changed at any time. Strong passwords, forced interval password changes are available as security settings. We log all account login attempts, and account lockout policies are enforced after a certain number of failed login attempts.

Physical Security

Our servers are in a Tier II/III high security dedicated data center located in the United States and monitored 24/7. Access is strictly monitored through card key protocols. Data center facility has a dedicated power feed. Electrical systems are protected by fully scalable 3-phase Uninterruptible Power System (UPS) with automatic failover, checking and monitoring systems. In the event of a full-power outage, automatic backup generator power is provided. Multi-redundant HVAC system.

24/7 Support

Our systems operations team monitors the the network 24/7, and engineers are available at any time in the event of an emergency.

Data Privacy

Customer and client data will never be shared with anyone. We will not share the personal schedule information of customers except with the client creating the schedule. All scheduling and appointment information will be confidential. Each customer can view only information relating to the customer's own account.

All our clients are required to log in before they are provided with access to their account information. A unique username and password must be entered.

Technical or support staff may view your data in order to help with a technical problem or to provide customer support. Access to personal information is limited to the few employees that may need to provide support to your account.

Data backups are done daily.

Data Retention

We will keep your data as long as your account is active. Upon request we will remove all stored data.

HIPAA Statement

Our technology, security, and privacy policies comply with HIPAA standards. PickAtime software incorporates numerous features to assist in your compliance with HIPAA, and to protect patient/client information. The following technological safeguards are employed: timed auto-logouts, protected passwords, multiple user access levels, strong 128-bit secure SSL encryption, high-end physical server security, nightly backups.

PickAtime meets all HIPAA Security requirements listed in Sec 164.308 - Administrative Safeguards, Sec 164.310 - Physical Safeguards, and Sec. 164.312 - Technical Safeguards.