**Security FAQs**

1. **Where is my data stored?**
   All data that is shared with TherapyAppointment is stored and processed in North America. Servers and networks reside in US-based data centers within the Amazon Web Service (AWS) cloud. Core staff are located in the US and Canada. Third-party data processors that integrate with the TherapyAppointment portal are also US and Canada-based.

2. **Will your third party vendors access and sell my data?**
   Our Privacy and security standards extend to third-party relationships. TherapyAppointment conducts reviews of third party software and computing vendors to ensure that they satisfy compliance requirements and are equipped to provide a similar level of protection to customer content. All third party vendors that store, process, access, or manage PHI on TherapyAppointment's behalf are required to enter into a HIPAA Business Associate Agreement that extends the privacy and security standards required by the application.

3. **Is there risk of application downtime?**
   Servers and networks leverage redundant designs to maximize availability. All servers and networks are distributed across at least two AWS *availability zones* to limit the risk of application downtime. File and database content for our systems is replicated automatically by AWS across three *availability zones.*

4. **How often is my data backed up?**
   Customer content and other critical data is backed up nightly to Amazon-managed storage within the same region and retained for a minimum of 35 days. For *most* types of information, our team is able to perform a *point-in-time* restore from backup to any moment within the past month.

   In addition to these backups, TherapyAppointment replicates a secondary copy of all customer data in real-time to a geographically separate location to aid recovery in the event of a major failure or natural disaster.

5. **How is my data encrypted?**
   TherapyAppointment leverages industry validated encryption solutions to protect all data transmitted or stored by the system. Where possible, we leverage native AWS encryption, which is built upon strong foundations and has been vetted time and again by industry experts. To ensure security and enforcement of our policies, we retain control over keys that are used by AWS for encryption.

   All customer content is covered by at least one layer of 256-bit AES encryption. For some particularly sensitive types of data, secondary encryption occurs within the application before data is stored in our database.

TherapyAppointment enforces encryption of network connections between the user and AWS as well as connections between the different components of the system. The primary encryption protocol for network traffic is TLSv1.2 though we also rely on SSH and other industry standard protocols for administrative purposes. In all cases, we harden the encryption configuration against known weaknesses and vulnerabilities.

6. **What tools do you offer to secure my multiple users in my practice?**
   TherapyAppointment provides multiple job-based roles and permissions enabling practice owners to grant the right level of access to each user in their account. We require customers to assign unique users and passwords to each member of their team, while providing free accounts for non-clinical staff to encourage compliance.

7. **How do I enforce security and compliance for my staff?**
   Practice owners also have the ability and responsibility to configure and enforce security and compliance settings for their staff, including:

   - Automatically sign users out after a period of inactivity (up to one hour)
   - Require two-factor authentication
   - Disable accounts automatically after 90 days of inactivity

8. **Do you use AI?**
   We have no plans to use your clients' data for AI training. We can clearly see that doing so could have unintended consequences and potential lawsuits. However, we are researching how AI could make an experience better from a support level.