BrainCheck

At BrainCheck, we are fully committed to ensuring the security and privacy of customers' and patients' health information. In compliance with the Health Insurance Portability and Accountability Act (HIPAA) and HITECH Act, we have implemented comprehensive safeguards to protect the confidentiality, integrity, and availability of protected health information.

Physical Safeguards

To ensure the safety of ePHI, all data is stored securely offsite using various cloud providers. In addition, our offices and equipment are in a controlled and secure environment and protected from intrusion.

Administrative Safeguards

To ensure we are compliant with HIPAA and the HITECH Act, we have taken the following measures:

- Conduct regular risk assessments to identify and mitigate potential threats to ePHI.
- Employees undergo HIPAA training to understand and adhere to our policies and procedures.
- Designated a Security Officer to oversee our compliance efforts.
- Established Employee Sanctions Policy to account for any HIPAA compliance violations.
- Established formal practices for implementing security measures that protect information and guide the conduct of personnel concerning the protection of information.

BrainCheck

Technical Safeguards

To ensure we are compliant with HIPAA and the HITECH Act, we have taken the following measures:

- Utilize encryption to protect ePHI both in transit and at rest.
- Access to ePHI is controlled via multi-factor authentication and role-based permissions.
- Regular system monitoring and audits are conducted to detect any unauthorized access or potential security breaches.

Our security practices include, but are not limited to:

Security Management Policy

- Risk Analysis Policy
- Risk Management Policy

Workforce Security Policy

- Authorization and Supervision of Staff Procedure
- Workforce ePHI Access Authorization Procedure
- Termination Procedure
- Business Associate Policy

Security Awareness Training

- Security Training
- Password Management
- Oral Disclosures of PHI

Contingency Plan

- Backup Plan
- Disaster Recovery Plan
- Applications and Criticality Analysis

Business Associates

Device and Media Controls

- Accountability
- Disposal of PHI and ePHI
- Data Backup and Storage

Technical Safeguards Standards

- Policy Access Control
- Encryption
- Antivirus and Firewalls
- VPN Protocol
- Additional Safeguards Employed

Audit Controls

By implementing these measures, BrainCheck strives to maintain the highest data security and availability standards and fully comply with HIPAA regulations.

For any questions about our HIPAA Security practices, please feel free to contact your Sales Rep.