

Security Statement

Policy Statement

This policy sets forth information security standards for the protection of client information at Broker Builder Solutions LLC. Maintaining confidentiality and integrity of client information stored, processed, or transmitted at Broker Builder Solutions is a requirement of all personnel. This policy applies to information in any format including electronic and hard copy.

The security policy ensures that:

- Information will be protected against unauthorized access.
- Confidentiality of information will be assured.
- Integrity of information will be maintained.
- Availability of information for business processes will be maintained.
- All actual or suspected information security breaches will be reported and thoroughly investigated.
- Information security training is provided for all employees.
- Procedures exist to support the policy, including virus control measures, passwords, and continuity plans.

Physical Security/Data Storage

Customer data is stored in our primary offices located at 201 E. Academy Street, Fuquay Varina, NC. Access to our location is restricted 24 hours a day. Physical access control is provided to only those with key entry. The office is monitored with video surveillance. In case of a natural disaster, security also includes automated fire prevention and extinguishing systems. In addition, Broker Builder Solutions utilizes a HIPAA compliant version of Progress ShareFile as a method of data storage. ShareFile is a cloud-based Software-as-a-Service (SaaS) solution that enables BBS to exchange confidential data securely.

Data Retention

Broker Builder Solutions retains client data for seven (7) years in accordance with its data retention policy.

Data Transport/Exchange

Broker Builder Solutions uses Secure File Transfer Protocol (SFTP) and PGP encryption, when required, to securely exchange confidential information with clients and business partners.

Electronic Security/Data Integrity

All systems used to retain client-specific data are encrypted using Symantec's Endpoint Encryption powered by PGP technology. All data stored outside of the Benefits Administration software is stored using one of the following.

- HIPAA-compliant version of Microsoft 365 SharePoint where users are required to provide validation credentials to access client-specific information.
- HIPAA-compliant version of Progress ShareFile where users are required to provide validation credentials to access client-specific information.
- Streamline platform, where users are required to provide validation credentials to access client-specific information.

Revision History

Date of Change	Responsible	Summary of Change
November, 2022	BBS Policy Team	Removed verbiage regarding NAS drive as it is no longer in use
July, 2026	BBS Policy Team	Updated company branding, office address, cloud storage references, and security terminology.