Privacy and Security Safeguards

Last Modified on 11/11/2026 3:43 pm EST

NextStep Solutions (NSS) has implemented the following procedures to safeguard the privacy and security of data stored on hosted servers:

- Restrictive external firewall rules are used to lock down the type of traffic that can enter the hosted environment from the Internet.
- Communications between client workstations and the data center are SSL encrypted to protect PHI.
- We use restrictive firewall rules within the environment to group servers into separate networks based on their purpose (web/application/database) and segregate your data and operations from other clients'.
- Password complexity policies ensure strong passwords.
- The minimum number of personnel required for optimal support are given access to the server and related hardware.
- Security cameras monitor the hardware 24x7.
- The hardware that stores your data is protected by use of electronic card readers and/or biometric verification for access.
- Security patches are applied on a regular basis.
- We audit all successful and failed logon attempts.
- Your data is backed up and stored in a secure secondary location each week night. All off-site backups are encrypted (AES-256 which meets FIPS-140 standard).
- Unnecessary software has been removed from all servers to reduce the risk of interference with the operation of NSS and for additional virus protection.
- Policies have been applied to restrict the functionality available to end users on the servers hosting NSS. The policies isolate the practices from each other and from the operations of the server environment itself to reduce the likelihood of users making inadvertent (or malicious) changes to the environment.
- Our hosting facility is SSAE 16 certified.
- We have implemented a network level intrusion prevention system which helps reduce the likelihood that some types of attacks against the network will succeed.
- Antivirus is installed on all Windows servers.
- Host-based intrusion detection system is on selected servers.