



Security Information about LSSN

Server Security

The security of the Linehan Suicide Safety Net (LSSN) application was assessed by an external auditor with respect to all of the applicable requirements noted in the Health Insurance Portability and Accountability Act (HIPAA) and HITECH federal regulations for the collection and storage of electronic protected health information. The LSSN application was determined to adequately mitigate against risks as required by these federal regulations. Specific security features of the LSSN application include:

Security information for the User:

- ✓ Users are assigned unique IDs to access the system.
- ✓ User passwords meet minimum length requirements (must be between 8 characters and 128 characters) and expire after 90 days.
- ✓ Five invalid attempts to log in to the application result in the account being locked out.
- ✓ Users are automatically logged out of the application after 15 minutes of inactivity.

Security information for the Company:

- ✓ Roles and associated capabilities for Behavioral Tech and Behavioral Tech Research staff are clearly defined and documented.
- ✓ Electronic data exports from the application are restricted to reports that do not contain any personal identifiers.
- ✓ Data transmitted to the application utilizes strong encryption algorithms to secure the data during transmission.
- ✓ Changes to the application are logged, tracked, and properly documented.
- ✓ Patient data is maintained for a minimum of 7 years, even if an LSSN subscription is suspended.

The LSSN server system is hosted and supported by a HIPAA-secure hosting service that complies with all US regulations and security standards regarding the storage of protected health information.



Please contact us at info@behavioraltech.org if you require additional information about the security of LSSN, and we will work with you and our hosting provider to prepare what you need.

Using LSSN Outside the United States

LSSN has been assessed by a third party for compliance to HIPAA regulations in the United States. At this time, it has not been assessed by any entity for compliance outside of the US and, as a result, may not be in compliance with local health data protection requirements for any international location. Requirements for capturing and storing protected health data are technical and complex, and while we hope to offer greater assurance to our customers outside of the US in the future, we are not currently able to do so.

Account Access

What happens if an employee leaves an agency?

In the event that an agency purchases one or more LSSN licenses and a staff member's employment is terminated by the agency or the employee, Behavioral Tech will deactivate that account upon request. If desired, an agency can have a new employee create a new account, and then request Behavioral Tech to activate pro-rated access for that account (i.e., the remainder of the subscription that was paid for on the pre-existing account will be applied to the new account).

If the agency needs access to the client LSSN files created by the departing employee, it is the agency's responsibility to recover that information prior to deactivating the account. Agencies can choose to have the departing employee share clients with other team members, and/or the client information can be exported in PDF format.

Behavioral Tech is not responsible for determining who should have authorized access to clients' protected health information. Requests to reactivate a deactivated account will be handled on a case by case basis.

Password Security

Per regulations to make LSSN compliant to HIPAA standards, you will be prompted to change your password every 90 days. It is your sole responsibility to:

1. Keep your passwords private and unknown to other individuals.
2. Set a secure password that meets the program's requirements and your agency's security requirements.
3. Promptly inform Behavioral Tech if you believe your account or password has been compromised, or if there is any other reason you need to deactivate your account.
4. If you attempt to you are unsuccessful logging into your account after 5 attempts, the system will lock you out for 24 hours. You will be unable to log into your account until this 24 hour period has expired.



Logging Out

The LSSN site will automatically log you out after 15 minutes of inactivity. If you leave your computer, tablet, or smartphone unattended for any reason, it is your responsibility to ensure that you've successfully logged out of your LSSN account by fully closing the entire web browser. Save any work before you logout.

Please note that if you have opened multiple tabs in the same browser, you must either close ALL the tabs of that browser or press the “**Logout**” button on the LSSN site for an account session to end.

For example, if you have 2 Firefox tabs open, one for using Suicide Safety Net and one for other activity, you will NOT be logged out of LSSN if you simply click the “X” on the Firefox browser to close the tab housing LSSN. However, if you were to close the entire Firefox browser, OR click the “Logout” button within the LSSN application, you will successfully end your LSSN session.

Behavioral Tech Contact Information

Phone: 206-675-8588

Email: info@behavioraltech.org

www.behavioraltech.org

Behavioral Tech Research Contact Information

info@btechresearch.com

<http://www.btechresearch.com/>