Springbuk® Privacy Statement

It is important to keep our user and client data secure. Additionally, HIPAA and other regulations require us to take careful precautions with client data is secured and protected. Below is an overview of the actions taken to ensure that that user data is protected from unauthorized use.

HIPAA Privacy Rule

Your privacy is ensured because only authorized users are allowed access to the system (see below). The system does not display data at an individual level. Additionally, we will never disclose individually identifying Protected Health Information (PHI) without your consent.

HIPAA Security Rule

The data in Springbuk is secured with a variety of techniques and controls. First and foremost, your data is encrypted during transmission from 3rd-party data providers to us, and is kept in an encrypted state when at rest within our system. During data processing, all personnel and programs needing to access this data must have the required decryption keys and access to even be able to access the data. The process for allocation of user accounts and decryption keys is controlled internally and according to our written operating procedures.

Additionally, the website has various levels of user access and roles, and only certain types of users (acting within their individually authorized accounts) are allowed to perform certain operations to query or otherwise process the data. Users must sign into our site via a secure HTTP connection (HTTPS), which prevents unauthorized users from intervening and seeing the data while it is being transmitted.

Our entire server environment runs in a secured, private network in the cloud, access to which is granted only to authorized employees (also according to our written operating procedures). In setting up the server environment, we have followed the cloud provider's documented best practices for ensuring direct access is properly configured.