fitabase

Security and Privacy Information

As a research platform that collects data from internet connected consumer devices, we take security and privacy seriously. Fitabase is a fully hosted, cloud-based software solution that implements robust industry standards to maintain secure databases and keep data private.

Where Data is Stored

Fitabase code and databases physically reside on the Microsoft Azure platform (www.windowsazure.com). We rely on the robust security, both physical on- premise guarding, and over network, provided as part of that platform. From Microsoft (http://www.windowsazure.com/en-us/support/trust-center/security/):

> *Windows Azure runs in data centers managed and operated by Microsoft Global Foundation Services (GFS). These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored, and administered by Microsoft operations staff that have years of experience in delivering the world's largest online services with 24 x 7 continuity.*
>
> *In addition to data center, network, and personnel security practices, Windows Azure incorporates security practices at the application and platform layers to enhance security for application developers and service administrators.*

Compliance

See information on Microsoft's extensive compliance at:
https://azure.microsoft.com/en-us/support/trust-center/compliance/

Offsite Backup Handling

In addition to the primary copies of our databases, Small Steps Labs LLC maintains snapshot archives of database for disaster recovery purposes. Backup copies reside on hardware only accessible to Small Steps Labs LLC and our employees. Our backup copies are encrypted and password protected.

See information on Microsoft's extensive compliance at:
https://azure.microsoft.com/en-us/support/trust-center/compliance/

Encryption & Secure Connections

Fitabase uses Secure Sockets Layer (SSL) for all authentication (logins), billing, and administration of the site. The user's browser establishes the authenticity by requesting an SSL certificate that verifies the identity of Fitabase. Once that SSL certificate is recognized, a Secure Sockets Layer (SSL) connection is established for security, encrypting data transmitted between browser and web server.

Passwords

Fitabase stores passwords in encrypted form. When an administrator attempts to log in to Fitabase.com, their attempted password is encrypted and if matched, the user is allowed in to the site. This practice prevents unauthorized usage of the site. If the database were to be compromised, passwords would not be retrievable.

Usage Logging

Fitabase logs all site usage, including attempts to access restricted data, or log in to accounts of others. We maintain security policies to block / freeze accounts that appear to be compromised until we are able to make contact via the email address used to set up the administrator account.

Optional Anonymous Data Collection

Fitabase allows groups wishing to collect data anonymously the option to do so by associating device data with their own alphanumeric identifiers. To best accomplish this, groups should set up the Fitbit.com account that corresponds with each device using an anonymous email address not linked to a real person. Fitabase does not collect personally identifiable information beyond what it is provided by Fitbit.com. Additionally, Fitabase does not collect IP addresses from synced participant devices.

Data Collected

Fitabase stores information provided to it by the Fitbit API (dev.fitbit.com). This information about:

- Physical intensity classification
- Number of steps walked
- Calories burned
- Sleep length, movement, and quality
- Heart Rate
- Type and duration of tracked and classified physical activities
- Weight
- Percentage of body fat
- Food logged

Data is stored and indexed in the Fitabase SQL Server database in day total, hour, minute-by-minute intervals, and second-by-second intervals (when available). Our database servers are IP firewalled and whitelisted such that they refuse any connection from IP addresses not preprogrammed by us.

No GPS or other location information is collected.