# Privacy and Security Analysis

## Current System

The current system provides some level of security and privacy, but has a long way to go. Currently, personal trainers can only see their own clients, and clients can only see their own data, and all users must log in before using either application. Data is encrypted in transit from the server over HTTPS. However, data is not encrypted at rest on the device (except for as provided by the operating system – e.g. Bitlocker, FileVault, or Android Full-disk encryption).

The applications are transparent about the data they collect with a privacy notice available within the app.

There are a lot of issues with the current system from a security perspective,

Authentication has the below problems

* Basic email/password authentication system
* No specified password complexity requirements
* Single-factor authentication only
* No session timeout mechanisms mentioned
* No specified rate limiting for login attempts

Data handling has the below issues

* No specified encryption for data at rest
* No mentioned data retention policies
* Unspecified data backup procedures

## Improvements to be made

While the system follows some security and privacy best practices, there is a lot of room for improvement.

### Encryption

While data is encrypted in transit, it is not encrypted at-rest, meaning a threat actor that is able to access a mobile device’s storage could gain access to the user’s information. Additionally, passwords are stored in clear text on the server (i.e. not encrypted, hashed, or salted – just human-readable text) which leaves the user accounts open to compromise – particularly when coupled with the lack of authentication on the server.

### Authentication

The authentication method implemented is very basic and only authenticates the user at login. Future API calls are not authenticated in any way – meaning anyone could call the APIs from the server, and potentially steal another user’s data. Similarly, there is no protection against a user modifying the data in the device’s storage to have a different client ID or personal trainer ID, and therefore viewing details of another user in the app.

The below are some improvements we should make for Authentication

* Implement Multi-Factor Authentication (MFA):
* SMS verification
* Authenticator app integration
* Biometric authentication for mobile devices
* Password Security:
* Enforce strong password policies
* Implement password expiration
* Add secure password recovery process
* Salt and hash passwords using modern algorithms
* Session Management:
* Implement session timeouts
* Add automatic logout after inactivity
* Track and manage concurrent sessions

### Authorization

Without Authentication, there can be no authorization – or rather, all users are authorized to do anything.