Jackson Long
Jalan Rivers
Eric Wills

<p style="text-align:center">Ethical Concerns of a Fitness Tracker</p>

When looking at the fitness tracker that we made, there are a few areas of interest when it comes to data privacy and complying to the GDPR. The first is legal basis and transparency. This pillar essentially means that the user should be able to see how their data is used, and have a legal justification to be doing so. In our case, we are simply displaying data, and only allowing users to modify their own data. The next aspect of GDPR is data security. This means that there should be safeguards in place to protect user data and react when there is a breach or a leak. In our application, we have a simple user login/authentication that could probably use some work. Next, we have accountability and governance which relates to the ability to use data across nations/organizations. This doesn't apply to anything that we are doing. Last, we have privacy rights. This is arguably the most important. This relates to the ability for the user to have access to all of the CRUD operations. The bottom line is that they have control of their data, and can request that it be removed from our application at any time.

In addition to the simple user authentication, we could implement a way to make the data harder to tie to one user in the database. This way, we can have a backup if anyone gets access to the database. We could also make it so the data in the database is hashed in order to slow down an attacker if they were able to get access. Finally, and in line with the SQL injection lesson, we want to make sure there are protections in place in case an attacker just wanted to cause harm to the application so we should be able to sanitize the inputs.