I. Design & Implementation Evaluation

- Using AVL tree, also known as self-balancing tree and a dynamic data structure, the program is able to perform insertion and search with relatively good speed, with the time complexities of ***O(logN)*** in average, as compared to ***O(N)*** and ***O(1)*** respectively in linear data structures.

- As the name suggests, an AVL tree is self-balanced, meaning the heights of two subtrees of any given node differ by at most one. This defining factor differs it from a simple Binary Search Tree, which has complexities of ***O(N)*** in worst case scenarios, with this self-balancing nature, each operation is ensured to have ***O(logN)*** complexity in all cases.

- However, this structure proved to be problematic when ranking patients at the rate of improvement since they were already sorted in alphabectical order of patient's id. I came up with two possible solutions to this problem:
    - Create a new AVL tree and insert the patients from the old tree in order of their rank scores. Similar to Tree Sort, ***O(N logN)*** time complexity in all cases, since this is not a BST (***O(N^2)*** in worst case).
    - Create a list containing all patients (in no particular order) and Merge Sort them in order of rank scores. This sorting algorithm costs ***O(N logN)*** time complexity in all cases.

- Since we are not allowed to use built-in data structure, I decided to use the first approach.

- To rank patients based on their improvement after 5 days, I used the scores system. In this system, each "NONE" at the end of a day add 10 points to the score, "FEEDING STOPPED" reduces 1 point, "REFER DIETTITIAN" reduces 3 points from the score. By sorting the scores in *descending* order, patients with higher "NONE" count will be at the top (ascending), for each "NONE" count level, those with higher "REFER DIETTITAN" will be at the bottom (*descending*), and for each "REFER DIETTITAN" count level, patients is sorted in *descending* order of "FEEDING STOPPED" count.

- To store feeding data of each patient, I used a 3D list although built-in data structures are not allowed, I could not think of any other way. Each dimension of this list is another list, the first dimension specifies days, the second specifies hours and the third specifies feeds, grv readings and issues. Hence, to access a specific information, we simply need to input day, hour and index at which the information is located ([2] for feed, [3] for GRV, [4] for issue similar to the csv file). Example: feeding_chart[2][14][3] will return GRV reading at 14:00 on day 3.

-

II. Data Security

Nowadays, electronic records are becoming popular in the industry, making it easier and faster for healthcare workers to get ahold of patients' data and make quick diagnosis and decisions. Unfortunately, this has also created a new patient privacy and data loss concern, making a cyber attack no longer a matter of "if" but "when" it will happen to a facility.

Thus, data security has become a great concern in the healthcare industry, since a data breach can cost a hospital their reputation, huge financial losses, lawsuits from patients and heavy penalties according to GDPR law.

To prevent and deal with a data security breach, hospitals should apply some measures such as:

1. **Encrypt** both patient data and hardware used to access said data.
2. Perform **Impact Assessments** (article 35 of GDPR) to stay up to date on potential cyber threats and propose solutions to reduce them.
3. Invest in a **firewall** and **antivirus software**.
4. **Limit network access** to authorized personnel only.
5. Adopt technologies to **limit the damage** when attacks occur.
6. **Segregate networks** to **isolate an attack** and limit the intruder's access. Medical devices network should be separated from security cameras and offices equipments since they provide access point that could lead to patient data**.**
7. Employ **monitoring services** to identify vulnerabilities, uncover suspicious behaviour and block malicious activity.
8. **Protect mobile devices**, like tablets, from unauthroized access, since clinicians usually access patient's health records and acessments.
9. Under article 43, GDPR requires "appropriate data protection **training** to personnel having permanent or regular access to personal data." (with Binding Corporate Rules (BCRs)
10. Uninstall unecessary applications, wipe data from discared devies, and update software regularly to apply latest security patches.
11. Back-up data in case a cyber attack lock personnel out of current patients' data, making correct treatments difficult.