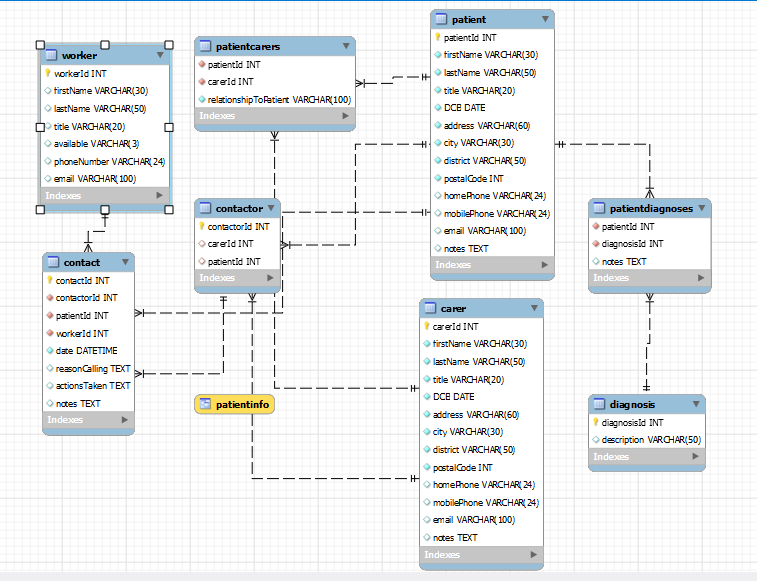
# Problem Statement

A client in the area of palliative care in the rural sector is concerned about the multiple potential contact points for patients and their carers. Examples of these carers could be. family, neighbours or friends. There is a desire for a system to ensure a single point of contact for the patients/carers. This point of contact would act as a triage point, and provide advice, refer the patient to a higher level of advice, or advise the patient to seek external treatment. This system would need to store information about the contact, including who called, who answered the contact, and the advice given or actions taken.

# ERD Diagram



**Reverse Engineering**

**Graphical user interface, application, email

Description automatically generated**

## Design decisions and normalisation

I believe that the **patient** must provide all the information, namely

* Full name and surname
* Date of Birth
* full address, including the region, as it is important to know if the patient lives in rural area.
* home phone, because patients are elderly, sometimes they reject technology, it is difficult for them to adapt to technology due to their advanced age.
* mobile phone
* email (who knows, maybe there are qualified IT specialists among the patients)
* notes - for more information

**Carer**

For the **carer** table, I decided that the following data would be needed

* Full name and surname
* Date of Birth
* Full address, including region and district
* Home phone
* Mobile phone
* Email
* Notes - for additional information

The **contactor** can be both a patient and a carer (if you remove all other persons who can call, but I believe that such persons will not be recorded). Table contactor should contain carerId and patientId. I think it is very important to specify that Contactor should be patient OR carer, I mean on what behalf caller is calling. Can it be a device? Like patient will have a button on special equipment (I am imagining a hospital bed with a button to call a nurse) to make call, if patient cannot talk for example. It will provide special message automatically which will contain just a patientId.

Table **worker** should contain standard information full name and surname, mobile(work) phone. An additional field that I believe should be present is the worker's availability, as it may not be available. At the moment it's Boolean, but maybe it's worth changing to two fields instead of one, one of them is the date of the available from, the other is available to. Additional information such as address, etc. I consider irrelevant in this situation, as it may be stored elsewhere.

**Contact** table has a contactID as a primary key, and contactorID, patientId, workerId as foreign keys referencing the corresponding tables. It has a date and time when the contact was made, what the reason for calling, actions that were taken and any additional notes if required.

**Bridging** table.

There is a bridging table called **PatientCarers**, which has patientId and carerId as both Primary and Foreign keys. The reason for creating this table was that a patient could have multiple carers, or one carer could look after multiple patients. This way, a patient cannot have only one foreign key of a carerId in its table, as it would create repetitive rows. The bridging table would deal with this problem and allow many-to-many relationship between Carer and Patient tables. This table also has an attribute that specifies in what relationship the carer and patient are.

**Diagnosis** table could be helpful to see the patient’s diagnoses during a contact. The table is normalized in 3NF and has no transitive functional dependencies. This table should contain diagnosis or disease ID and name or description of it.

**Bridging** table **PatientDiagnoses** is created in case a patient has multiple diagnoses. The table is normalized in 3NF and has no transitive functional dependencies. This table contains PatientID and DiagnosisID.

# Security and GDPR

**Privacy Act 2020 and the Privacy Principles** – looks very similar to me, it was not in my plans to violate these principles and laws. There is no point to dive deeper into Privacy act, because all information can be found there

https://www.privacy.org.nz/privacy-act-2020/privacy-principles/

## GDPR

General Data Protection Regulation (GDPR) is the European Union privacy law that came into force in 2018 and requires all the companies that hold or process the personal data of people residing in the European Union will be required to comply with the Regulation (Intersoft Consulting, 2020).

There is a possibility that some of the patients might be EU residents, so that is why the system should be compliant with GDPR. There is a lot of personal data (data, that can be used to identify an individual) stored in the database, such as: names, addressed, dates of births. There is a possibility that the database can store payment and banking information as well.

Complying with GDPR means having an obligation to (365 villas, 2018):

* Be clear about the lawful basis upon which you are storing or processing the personal data
* Only use the data for the purpose that the consent was given.
* Ensure to get an agreement, in a GDPR compliant format, from the individual for you to store the data, and communicate how you will process the data collected, including the rights of the individual to access, remediate or erase the data.
* If you are collecting personal data for more than one purpose, gain separate consent for each purpose and have a clear, audit-able process for recording (and storing) the date and method of consent.
* Only hold the data needed and only store it for as long as it is needed
* Keep the information secure and, in the event of a serious data breach, notify the ICO within 72 hours
* If you process the data of under 18’s, have systems in place to verify individuals’ ages and obtain parental or guardian consent for any data processing activity of individuals under the digital age of consent (in the UK the digital age of consent is 13 years old and over).

To make a database GDPR compliant, I will have to ensure the following steps are implemented:

* **Create and enforce roles and permissions.** By defining roles and permissions on the database level in advance, I can prevent unauthorized access to sensitive personal data.
* **Mask sensitive data.** Data masking within the database ensures that the developers and engineers can use real data when working on their databases, without compromising any individual’s privacy or breaching any articles of the GDPR.
* **Prevent data loss and alteration.** Maintaining the integrity of data is just as important as the security measures used to collect and store it. I plan on implementing hashing and encryption in the database.

## GDPR Compliance

In Iteration 1, the database was not GDPR compliant as it did not have any security measures implemented.

In iteration 2 security measurements were implemented. Roles and users were created, rights were assigned.

# Coding

### Iteration 1

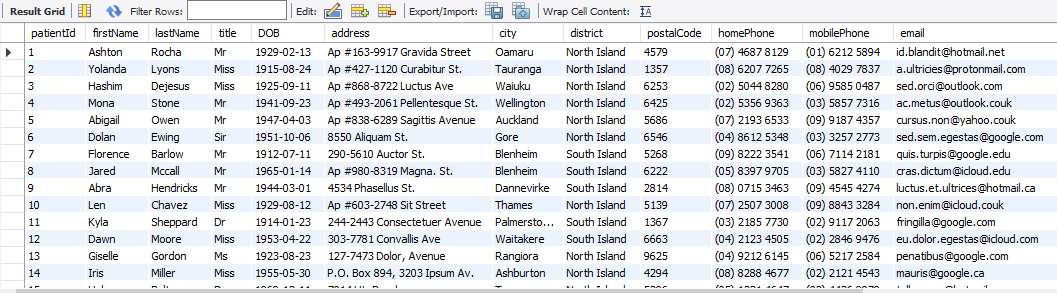
In Iteration 1, I implemented the following tables:

* Carer
* Patient
* Contactor
* Contact
* Worker
* PatientCarer(bridging Table)

I generated sample data on generatedata.com and inserted it into tables:

**Patient, Carer, Worker** tables I have filled with data by using a very simple tool Data Table Wizard Import,which is part of Mysql WorkBench!

**Patient**



**Contact**

Graphical user interface, application

Description automatically generated

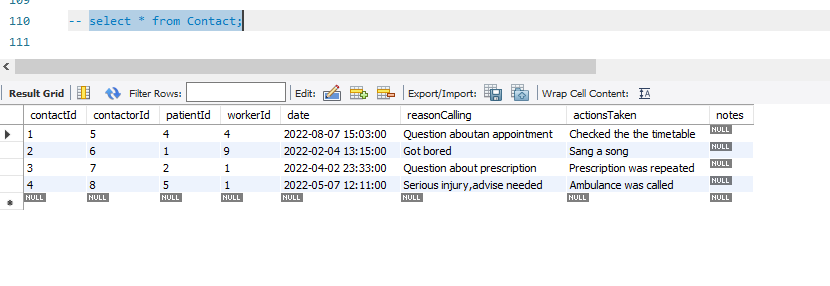
**Carer**

Graphical user interface, application

Description automatically generated

Unfortunately, I could not do the same for the rest of the table, due to tool restrictions. I had to do it manually by inserting data with a query.

**Contact**



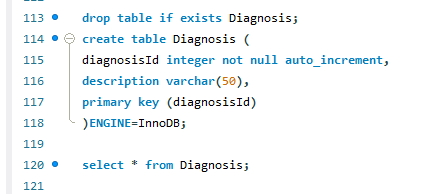
**Example of inserting**

Text

Description automatically generated

## Iteration 2

**Creating a Diagnosis table and inserting data**



**Inserting data**

Graphical user interface, text, application

Description automatically generated

**Creating a PatientDiagnosis table**

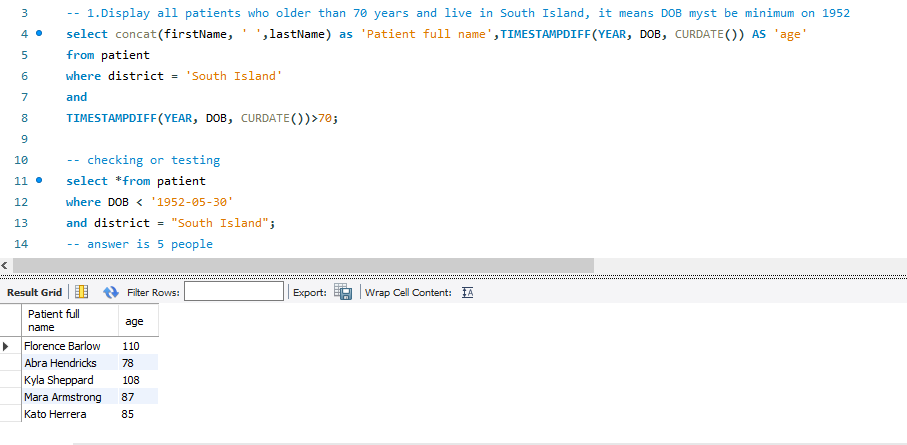
**Graphical user interface, text, application, email

Description automatically generated**

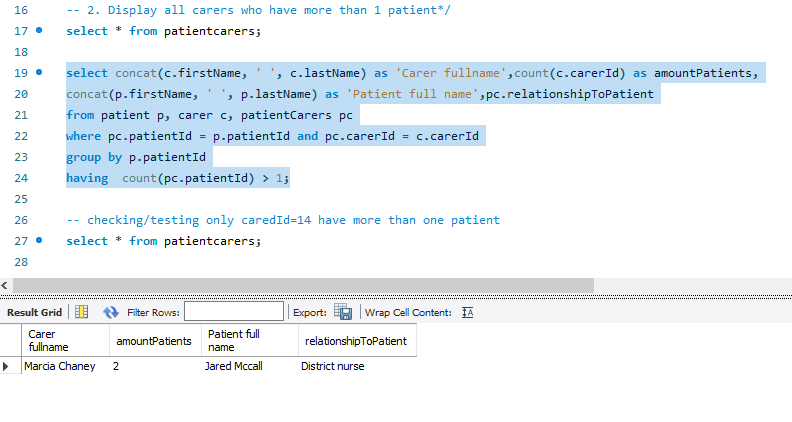
## **Queries**

## Iteration 1

Query 1. Display all patients who older than 70 and live in South Island

****

Query 2. Display all carers who has more than 1 patient



Query 3.Display how many times particular carer made a contact.

Graphical user interface, text, application

Description automatically generated

## Iteration 2

Query 4. Displaying important information about patient through a VIEW

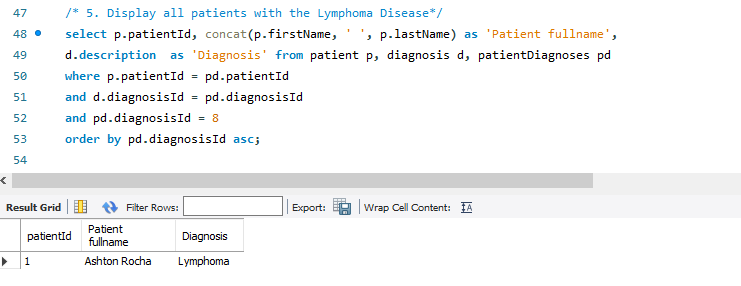
Graphical user interface, text, application

Description automatically generated

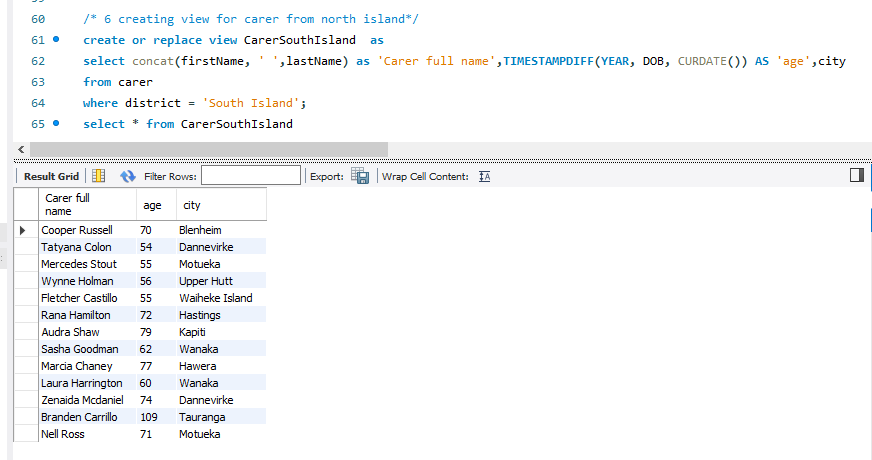
**Graphical user interface, table

Description automatically generated**

Query 5. Display all patients with a Lymphoma disease.



Query 6. Display all carers from North Island

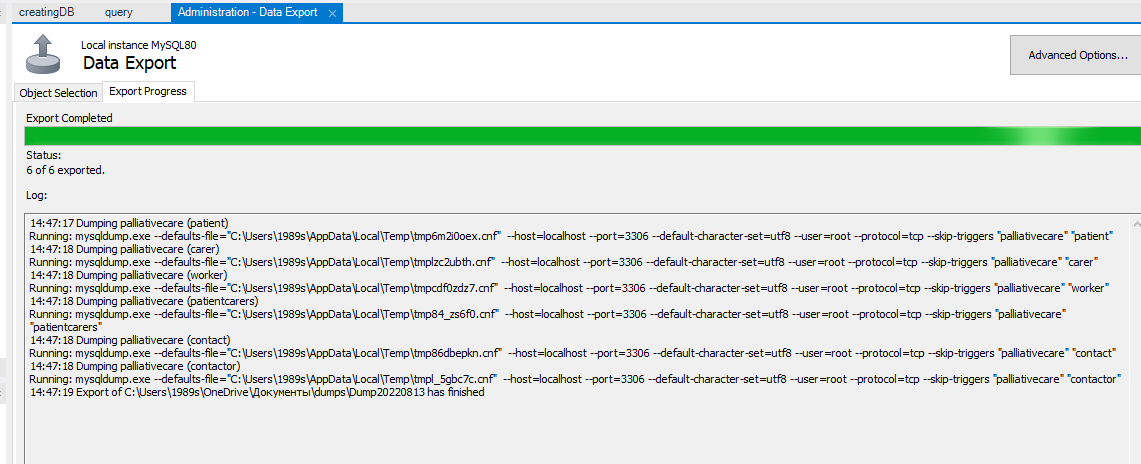


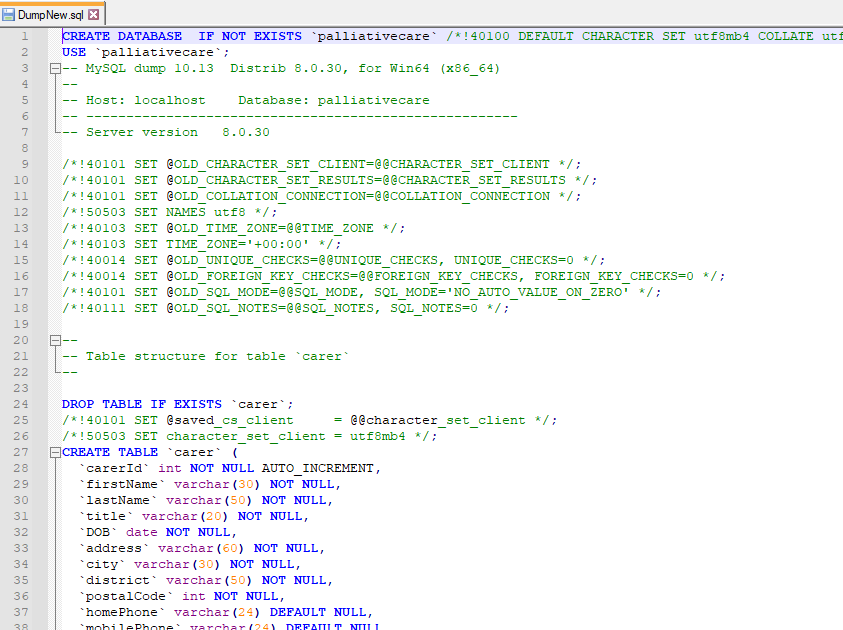
# Backup

A backup of all personal and general data should be made at the beginning, immediately after the information has been received, as unforeseen circumstances can happen at any time.

After I have created 2 new tables and inserted more data I must do a backup for my database.

**Prove of a backup**





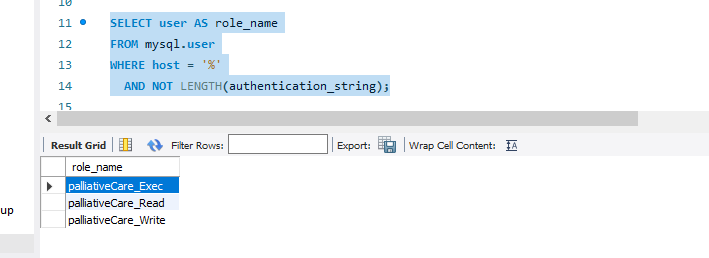
Unfortunately, my version of Mysql does not have a proper tool MysqlEnterpriseBackupRecovery.I had to export (dump it) it instead.

# Security/coding

**Creating roles for a database**

A picture containing text

Description automatically generated

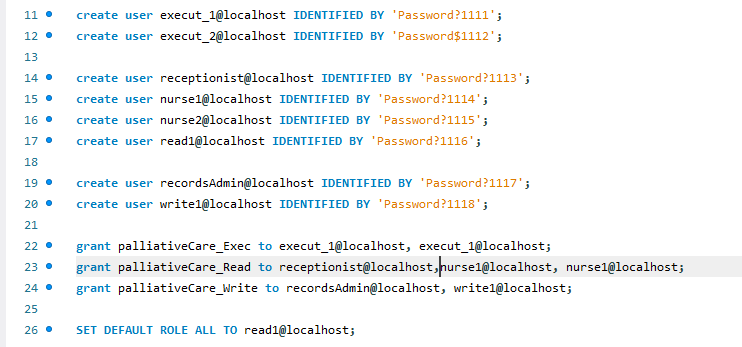


**Granting access rights to roles**

Graphical user interface, text, application

Description automatically generated

**Creating users and granting roles to them**

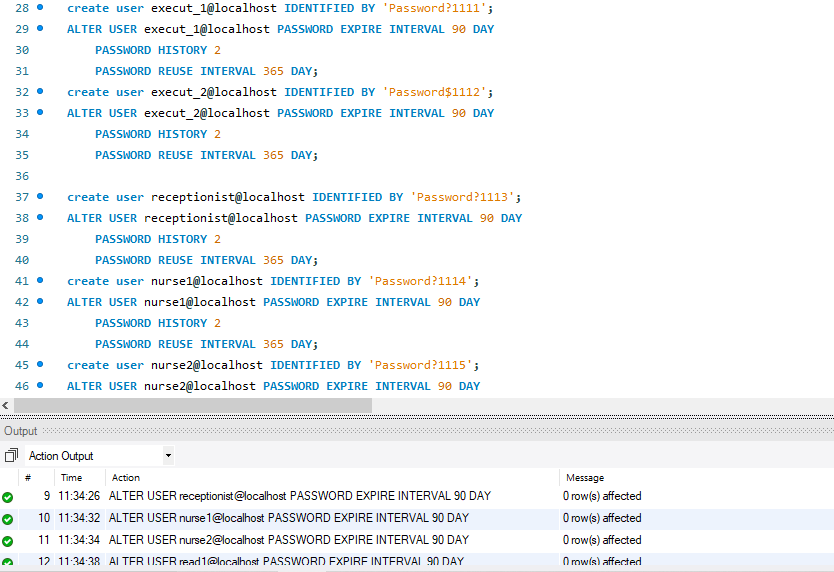


Prove

Graphical user interface, text, application

Description automatically generated

Creating a passwords and 90 days expiration of this password for an users, moreover users need to change a password twice per year.





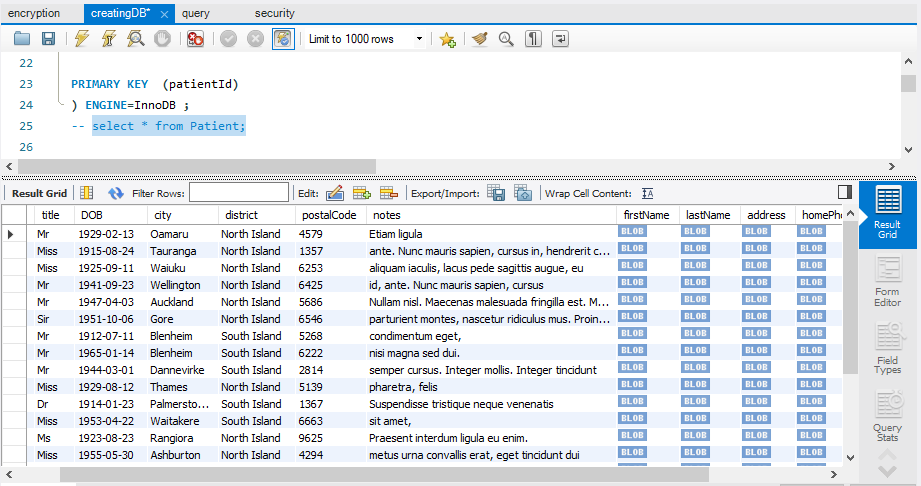
**Iteration 3**. Encryption

Creating encryption for a patient table

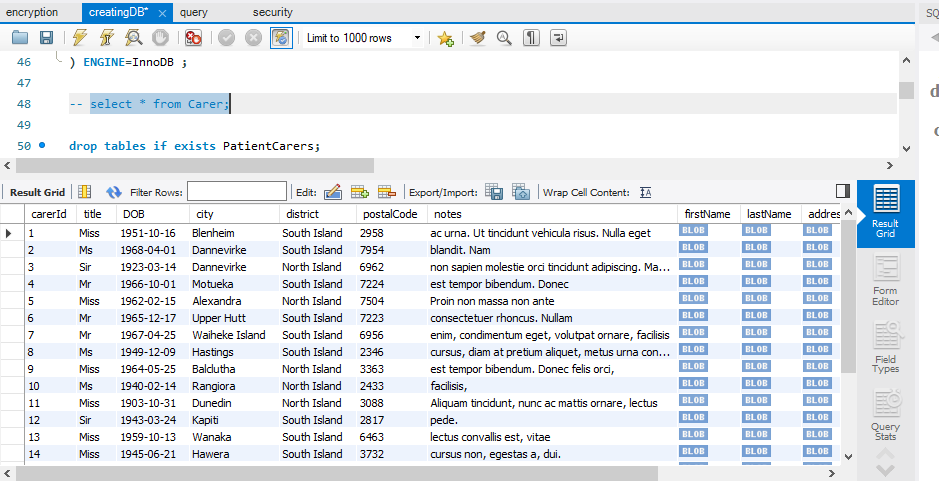
Text

Description automatically generated with low confidence

Select \* from patient table



Select \* from carer



Select \* from worker

Graphical user interface

Description automatically generated

# Evaluation

The hardest part is always getting started.

**Iteration 1** performance was satisfying. It was hard to divide all the work into equal iterations as some things like security or views are hard to do without fully implementing the database.

It was difficult to come up with a relevant field for tables, cutting off everything unnecessary and non-relevant. Since I have no experience specifically in this industry, it is quite possible that I missed some important information. I hope that in the next iteration I will correct my shortcomings.

For the future Iteration I am planning to secure all data, do a backup again and draw a normalization diagram.

**Iteration 2** was easier and quicker. I am happier with my database now. I have added two new tables and inserted more data. Now my database looks more complete, as I think it was missing diagnosis table. Obviously, I had to do a backup again, as a good practice. There are significant changes to security. The database is now more GDPR-compliant with the roles and user accounts created and assigned. In the next iteration, I plan to look into encrypting and creating more views and indexes to check queries for performance.

I have created two views which are perform faster and better than just queries.

**Iteration 3.**The performance in Iteration 3 was satisfying. Although I had some problems with finding out how to implement encryption efficiently, I managed to find some good tutorials that explained it step-by-step. Encryption took me a lot of time, as it is quite hard to do right in the end, in the future I should consider doing it at the same time as creating tables.

Now database is fully GDPR – complaint.