# GDPR Compliance

## How GDPR will affect my design.

The GDPR will force me to make sure that all the data that I might store is the same throughout all of the EU as I could potentially have services that I will be applying to someone that lives in the EU for example one of my clients being an EU resident. I will have to pay attention to what data I am choosing to store as I would not be allowed to store and show any data that could be used to identify a person and that is not relevant to my product.

Things that I must follow when I gather data that could identify a person is

* the data subject has provided consent to the processing
* the processing is necessary to protect the vital interests of the data subject or of another natural person

According to the EU General Data Protection Regulation General Information Document, the users of my product have rights when it comes to the collection of data.

* Right to information
* The right to be forgotten
* Right to restriction of processing
* Right to data portability

If I was not able to provide any of these features and rights, I would not be able to operate in the EU nor would I be able to conduct business with any one person that is currently in the EU I would be restricted to stay within New Zealand and do all my business here.

## How my solution will comply with GDPR.

What I will do to make my database comply with GDPR.

I will ask for consent of all the patients, carers and workers that will be inserted into the database and if the database needs to be tested it will be tested with data that is made up and not of any individual that is real. The data that I am storing is all necessary for the context of the business I am not storing unnecessary identifiable information, I am not storing patient NHI numbers or phone numbers this is the same for all carers and workers.

### Consent

consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes.

### Right to information

I will inform all clients on how I am processing the data and what I am doing with the data.

### The right to be forgotten

If any of my users want their data to be removed, I will do that.

### Right to restriction of processing

I will allow for users to restrict some of the data that I am collecting.

### Right of data portability

I will use a common readable format when exporting the data so that the client can see the data if they request it.

# Data breach notification

It is mandatory to notify all users of a breach when one occurs, this breach cannot take longer than 72 hours after becoming aware of the breach.

# Security

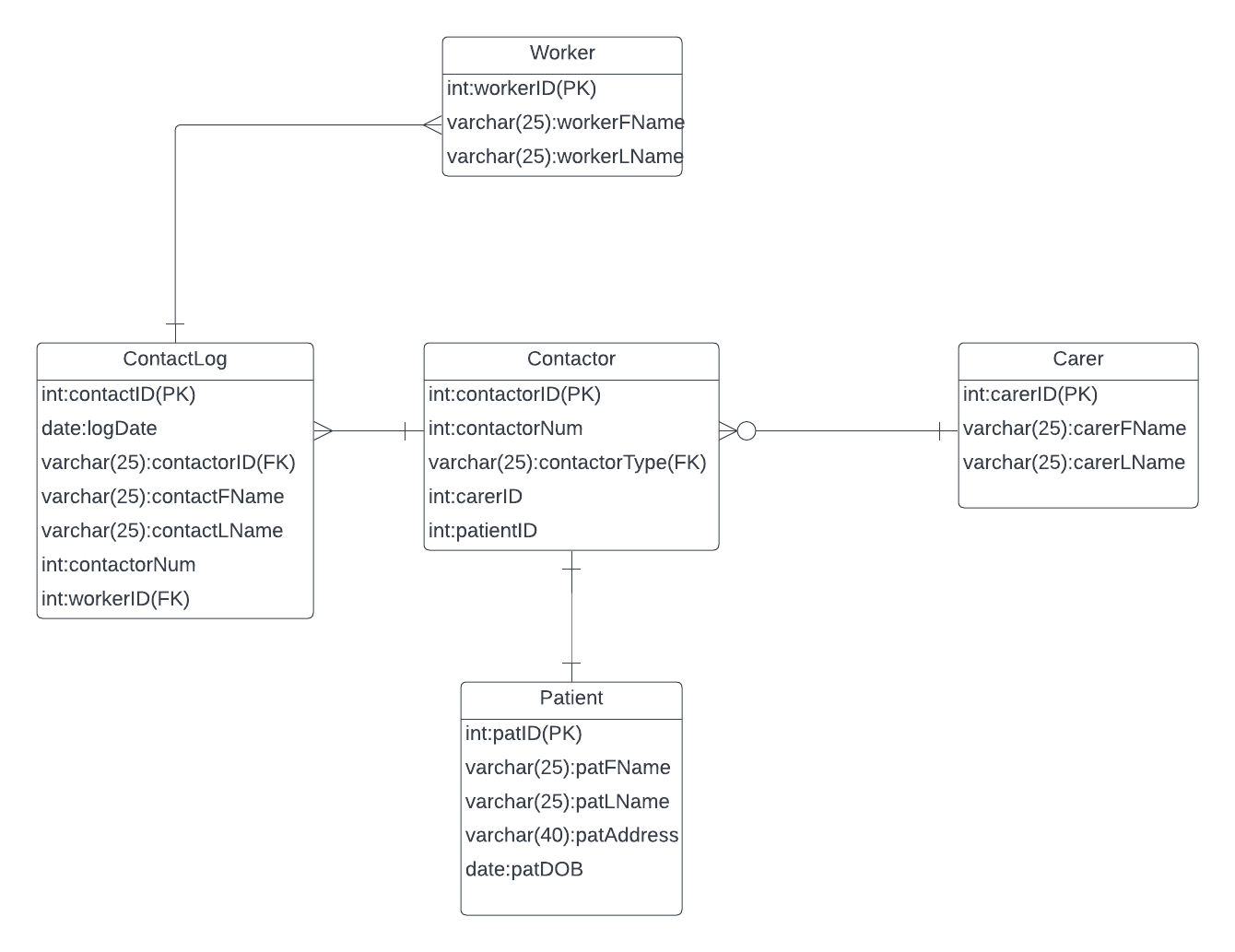
For security reasons the worker will only be able to access the contact logs generated when a patient or a carer makes a contact, this is to ensure that the worker is only seeing specific data and cannot see any identifiable information from the patient and carers, this data would include the carer and patient contact details and addresses of the patient and cares.

The patient and carer will have access to their own information and each other’s information as they must be in contact with each other.

# Backup

We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. I will store multiple backups and store them in different locations to prevent losing all data in the database

# ERD



# Normalization

# NF2