NUS
National University
of Singapore

CS3205 Information Security Capstone Project

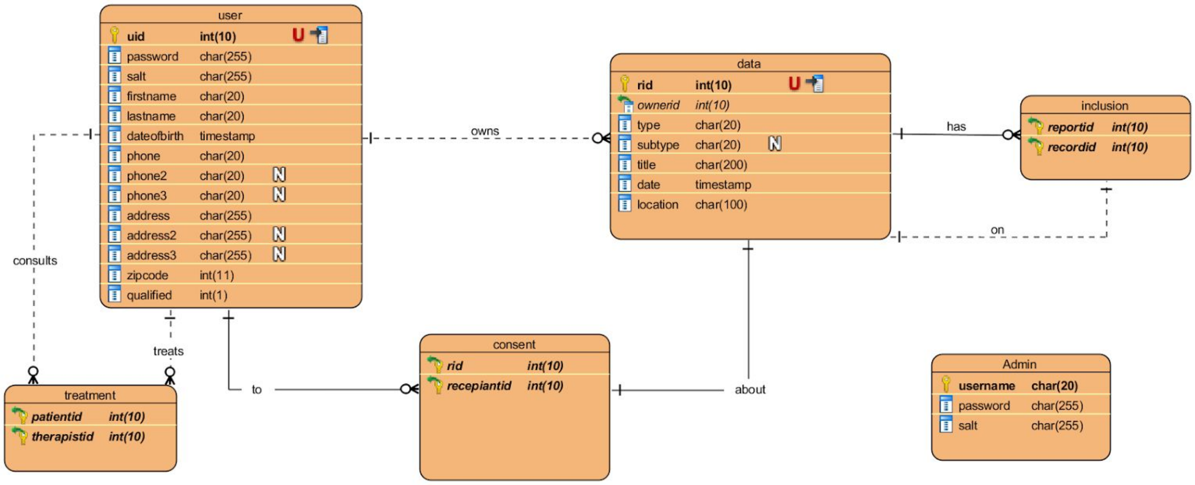
Semester 1 2017/2018

Database Functional Specifications

Team 1	Name	Student #
Member #1	Ang Kiang Siang	A0125528E
Member #2	Cao Wei	A0144422R
Member #3	Chai Wai Aik Zander	A0076510M
Member #4	Choo Rui Bin	A0124636H
Member #5	Chua Li Qun Shawn	A0129612J

1 Entity Relationship Diagram

The entity relationship diagram of the system is as below:



2 Database Schema

User Table

Attributes	Data type	Description of Fields	Remarks
uid	int(10)	Identification number for user	Primary Key
password	char(255)	Message digest of user’s password	Not Null
salt	char(255)	Salt for hashing the password	Not Null
firstname	char(20)	First name of user	Not Null
lastname	char(20)	Last name of user	Not Null
dateofbirth	timestamp	Date of birth of user	Not Null
phone1	char(20)	Primary contact number	Not Null
phone2	char(20)	Secondary contact number	Nullable
phone3	char(20)	Secondary contact number	Nullable
address1	char(255)	Primary address of user	Not Null

address2	char(255)	Secondary address of user	Nullable
address3	char(255)	Secondary address of user	Nullable
zipcode	int(11)	Zip code of user’s address	Not Null
qualify	int(1)	Whether user is a therapist	Not Null

Treatment Table

Attributes	Data type	Description of Fields	Remarks
patientid	int(10)	Identification number for the user as the treated patient	Primary Key, References to user (uid)
therapistid	int(10)	Identification number for the user as the therapist	Primary Key, References to user (uid)

Data Table

Attributes	Data type	Description of Fields	Remarks
rid	int(10)	Identification number for the medical data	Primary Key
ownerid	int(10)	ID of the owner of this record	References to user (uid)
type	enum (“Readings”, “Images”, “Time series”, “Movies”, “Document”)	Type of the medical data (E.g. Readings, Images, Time series, Movies, Document)	Not Null
subtype	char(20)	Subtype of the medical data(e.g. Blood pressure readings, MRI or therapist note)	Nullable
title	char(200)	Title of data	Not Null
date	timestamp	Date recorded of the data	Not Null
location	char(100)	Absolute path of the data stored	Not Null

Inclusion Table

Attributes	Data type	Description of Fields	Remarks
reportid	int(10)	Identification number for the medical report	Primary Key, references to data(rid)
recordid	int(10)	Identification number of the medical record associated	Primary Key, References to data (rid)

Consent Table

Attributes	Data type	Description of Fields	Remarks
rid	int(10)	Identification number for the medical report	Primary Key, References to data(rid)
recipientid	int(10)	Identification number of the recipient therapist	Primary Key, References to user(uid)

Admin Table

Attributes	Data type	Description of Fields	Remarks
username	char(20)	Username for the admin	Primary Key
password	char(255)	Message digest of user’s password	Not Null
salt	char(255)	Salt for hashing the password	Not Null

3 Activities

The possible activities that can be undertaken by the users of the system are listed as follows.

1. A user can update his own particulars on a management page, with the information being transmitted to the server using a POST method.
2. A user can upload his records on his profile page. Only a few extensions (e.g. doc, pdf, mp4) are supported.
3. A user can view / download his records (i.e. images, videos, medical data, etc.) via the web page.
4. A user can select a qualified user to be his therapist on the latter user's profile page.
5. A therapist can view his list of patients and patients can view his list of therapists.
6. A therapist can view his list of notes regarding a certain patient he treats.
7. Users can give consent to other users to view data that he owns on another management page, subjected to the following rules:
    a. A patient can give consent to his therapist to view his medical report.
    b. Similarly, a patient can also revoke a current therapist's access to his medical report.
    c. A therapist can give consent to a patient to view notes about himself.
    d. A therapist can give consent to another therapist to view notes about one or more patients, **if the other therapist has consent to all the data included in the note**.
8. Admins can add / edit / delete users on a special management page. Admins' credentials will be stored in a separate table.

4 Rules

Here are some proposed rules for the database system. Since this is a preliminary design report, these assumptions and axioms have not been fully tested for consistency. Detailed examinations and proofs will be included in the design report.

1. A user cannot be the therapist of his own.
2. A data cannot include its own.
3. A therapist note (report) on a patient can only be created by one of the patient's therapists.
4. A consent of data other than a therapist note (report) can only be given to the owner's therapists and no one else.
5. A consent of a therapist note (report) can only be given to another therapist who has access to all the data the therapist note (report) includes.
6. An inclusion of a therapist note (report) implies the inclusion of all the data that therapist note includes.
7. When a consent about a data to a therapist is revoked, the consent about all the other therapist notes (reports) containing this data to that therapist shall be revoked.