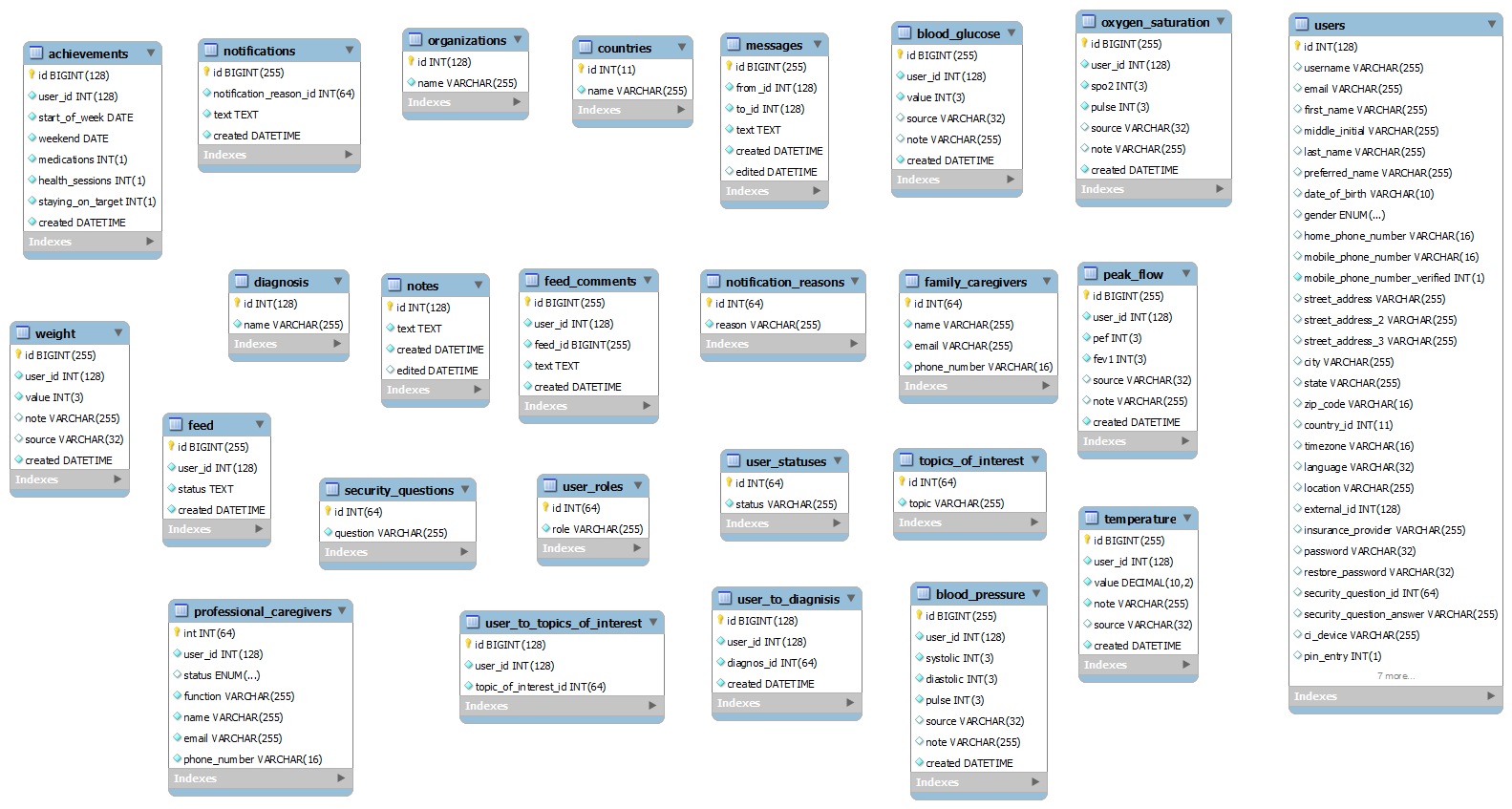
# Database structure

Initial database structure can be found below.



\* Please note, this diagram doesn’t represent relations between database tables and indexes.

\*\* Some field types may change during development and depending on security solution we will choose.

# Security

## Three-Tier Design

This design incorporates the three layers of a Web application running on different servers, usually set apart by firewalls that have specific rules to only let traffic through to the specific port on a specific server at whichever layer that the user is trying to access:

Internet -> Firewall -> Web -> Firewall -> Application -> Firewall -> Database.

## Access Control

Access to information contained in the tables must be properly regulated. This can be done with control over direct access to the tables, and also through views. Views and privileges assigned to the views can be created to limit users to only see specified portions of data contained within a table.

## MySQL AES encryption

To encrypt & decrypt MySQL data AES\_ENCRYPT() and AES\_DECRYPT() functions will be used. These functions use the official AES (Advanced Encryption Standard) algorithm & encode data with a 128-bit key length. Which is much faster and secure enough for most purposes.

Sensitive database field types will be changed to VARBINARY, BLOB or any other suitable types for storing encrypted values.

## Individual Keys for Providers

Each provider will receive it’s own key for encryption. Keys should be stored in files on server with read-only access for PHP scripts.

Secret Key will be passed to MySQL at the beginning of connection as a variable. For security reasons all further database queries will use it as show below:

SELECT AES\_DECRYPT(first\_name, @AES\_KEY), AES\_DECRYPT(address, @ AES\_KEY) from users;