**Udacity Health Privacy Assessment**

Student Name: Carlos Fernando Chicata Farfan

Date: 2022 may 21

# Executive Summary

There are several points need to improve about privacy in system. Those points are related with children, medical acts in focus of notification; consent, security and control access of data of user.

## Number of Findings

Total: 6

### Finding #1 missing the parents data in database to notify in children users case

**Detail Explanation:in database, there are users under 13 years; In COPPA said the parents need to get notification but the data do not explicitly indicate who is the parents and way to communicate him, only the child user. Example: 4 and 7 records in “patient-registration.db part 4”**

**Regulation(s) in question: COPPA**

**Recommendation: model and store in database, fields that indicate who is the father/mother and ways to communicate him/her,**

### Finding #2 Don’t get parental consent for children users

**Detailed Explanation: in document of specification. Doesn’t indicate the process to get a parental consent in case of childre user registration in system. Also don't store any data associated this process.**

**Regulation(s) in question: COPPA**

**Recommendation: explain in specification document of app; how is this process and where in database store this data to show the those type of users are supported by parents**

### Finding #3 Analytics team don’t need get access all data

**Detailed Explanation: in specification document indicate that analystcs team get access to all collected data of user in database to calculate active usage. But they don't need to get access to all data; fields like first and last name or home address don't need to use to calculate active usage in users. So need to get better control of access of users.**

**Regulation(s) in question:HIPPA**

**Recommendation:** **in different teams get differents levels of access in data to work.**

### Finding #4 don’t download information to doctor’s device

* **Detailed Explanation: the specification document indicated that “Doctors have the capability to download their patients data to their personal devices”, it is violated into the physical safeguard in point of the restriction of access in mobile device., lost control of access data of user.**

**Regulation(s) in question: HIPAA**

**Recommendation: show user data that doctor will use in web system.**

### Finding #5 don’t get consent document to research using data

**Detailed Explanation: in specification document indicated “Udacity Health has prepared a data set to send to a research company. The set of data will be anonymized “ but in nowhere indicate the authorization of the user that you will use his data for this specified purpose. Violated the consent of data usage.**

**Regulation(s) in question: HIPAA**

**Recommendation: generate and store data about the consent of usage data in research of users. Create a process to get and renovate this consent.**

### Finding #6 don’t encryption in rest in all part of architecture software

**Detailed Explanation: in specification document indicated that HTTP protocols to communicate components in architecture system. It’s violated the technical safeguard of security rule of HIPAA.**

**Regulation(s) in question: HIPAA**

**Recommendation: using HTTPS to communicate backend and database inside of architecture system in the cloud provider**