**Udacity Health Privacy Assessment**

Student Name Masanori Fukuhara

Date September 8, 2022

# Executive Summary

The following is a list of improvements that can be made to protect patient privacy and maintain a healthy healthcare business.

Consideration should be given to limiting the use and disclosure of patient data to the minimum necessary, or to anonymizing and protecting patient data privacy before using it for AI. (HIPPA-Privacy)

Improvements are needed in transmission security and access control, which are technical safeguards, and device security, which is a physical safeguard, to ensure the secure operation and storage of patient data. (HIPPA-Security)

When collecting and storing data limited to those necessary for medical treatment, due consideration should be given to security and to ensure that consumers (patients) are not disadvantaged. (Article 5(a) FTC Act)

## Number of Findings

Total: 6

### Finding #1 **Limiting Uses and Disclosures to the** **Minimum Necessary**

**Detail Explanation:**

1. **Limiting Uses**

Regarding the following statement in the specification

“Udacity Health Analytics team has access to all data collected from the users. They will use the data to calculate monthly and weekly active usage. “

It is not necessary for the entire team to have access to all patient data in order to calculate monthly and weekly active usage. The person in charge of calculating monthly and weekly active usage should be designated and should have access to the minimum amount of data necessary to perform his or her job.  
  
  
For internal use, covered entities should develop and implement policies and procedures that restrict access to and use of protected health information based on the specific roles of members of the workforce. These policies and procedures must also identify the individuals or classes of employees who need access to protected health information to perform their job duties, the categories of protected health information requiring access, and the conditions under which access is required.

1. Minimum Necessary

Some of the information we currently collect may contain information that is not inherently necessary for the performance of medical treatment or services

“

Data Collected form User

* First Name
* Last Name
* Phone number
* Home Address
* IP Address
* Ethnicity
* Gender
* Medical History
* Age
* Work History
* Credit Card Data

“

**Regulation(s) in question:**

[Minimum Necessary Requirement | HHS.gov](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html)

45 CFR § 164.502 - Uses and disclosures of protected health information: General rules.(b)

45 CFR § 164.514 - Other requirements relating to uses and disclosures of protected health information

(d)

**Recommendation:**

* Define the team or person in charge of calculating monthly and weekly active usage, identify the minimum data required for the person in charge to perform his/her job, and grant the person access to only the target data.
* The data to be collected should be limited to the minimum necessary data. If data is necessary, the reason why it is necessary should be clearly stated.

### Finding #2 　 **Technical Safeguards**

**Detailed Explanation:**

1. **Transmission Security**

Regarding the following statement in the specification

All communication between the servers and databases in the Udacity Cloud environment uses HTTP.

A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.2

1. **Access Control.**

Regarding the following statement in the specification

* Only 1 pop-up on the page which is to chat with a health professional
* Menu items on the page are to:
  + - Schedule
    - Pay
    - FAQ
    - Contact Us

**Schedules and Pay are information that should be accessed through personal authentication**

A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).24

**Regulation(s) in question:**

45 CFR § 164.312 - Technical safeguards.(e)

<https://www.law.cornell.edu/cfr/text/45/164.312>

* Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
* Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

**Recommendation:**

* Encrypted communication: Communication is done over HTTPS, and encryption prevents unauthorized intrusion from the outside from detecting the contents of the communication.
* Allow access to personal information via personal authentication. Apply multi-factor authentication to eliminate as many opportunities as possible for spoofing and unauthorized access.

### Finding #3 　 **consumer privacy**

**Detailed Explanation:**

1. **consumer privacy**

It is not reasonable to collect a consumer's occupation, title, income, or credit information in the course of medical practice. If the collection of data were necessary to The collection and storage of such information without due consideration for security may cause serious damage to consumers, which consumers cannot reasonably avoid, and may result in transactions that are disadvantageous to them.

**Regulation(s) in question:**

Consumer Privacy Regulation　Section 5(a) FTC Act

<https://www.ftc.gov/about-ftc/mission/enforcement-authority>

**Recommendation:**

Minimum Measures

* Adopt a multi-layered approach to security. Place multiple safeguards on protected information.
* Take extreme care to address security concerns as soon as they arise
* Due diligence to continuously monitor and investigate potential security concerns

### Finding #4 　Physical Safeguards　.

**Detailed Explanation:**

1. Workstation and Device Security

Regarding the following statement in the specification

Doctors have the capability to download their patients data to their personal devices.

 covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media.22 A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).23

**Regulation(s) in question:**

45 CFR § 164.310 - Physical safeguards.

<https://www.law.cornell.edu/cfr/text/45/164.310>

(c) Standard: Workstation security.

**Recommendation:**

Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

### Finding #5 　de-identified information for AI use

**Detailed Explanation:**

1. Ai for health care

The scheduling system will use AI to give preferable times. The AI model will use users profile data (Name, Race, Age, Gender, Address) and medical record to determine who has the most critical need.

Consideration should be given to providing data to third parties in building AI models, and data should be limited to the minimum necessary for AI models. In providing data to third parties, restrictions on the use and disclosure of health information should be lifted by removing personally identifiable information and anonymizing the data so that it cannot be matched with other information.

**Regulation(s) in question:**

[HIPAA and Machine Learning AI Compliance Software (compliancy-group.com)](https://compliancy-group.com/hipaa-compliance-and-ai-solutions/)

45 CFR § 164.502 - Uses and disclosures of protected health information: General rules.

<https://www.law.cornell.edu/cfr/text/45/164.502>

45 CFR § 164.514 - Other requirements relating to uses and disclosures of protected health information.

<https://www.law.cornell.edu/cfr/text/45/164.514>

**Recommendation:**

* Limit the data to the minimum required for the schedule proposal model, and anonymize patient and health information to train the AI model by processing the data in a way that does not identify individuals.
* Remove information (Race, Gender) not needed for the schedule proposal model.
* Personally identifiable Name is replaced with ID, and medical records and addresses matched with ID are anonymized and used for the AI model. The medical record and address are anonymized and used in the AI model.

### Finding #6 Access of individuals to protected health information

**Detailed Explanation:**

1. Access of health information

Regarding the following statement in the specification

Data Deletion

When a user deletes their account they are no longer able to access their account or account data. All data is retained in the system for perpetuity.

Data Export

* Only able to perform export on active account
* The user will get the following information in a .csv format when performing export
  + First Name
  + Last Name
  + Home Address
  + Medical History
  + Age
  + Phone Number

An individual has the right of access to inspect and obtain a copy of protected health information about the individual in the designated record set as long as the protected health information is maintained in the designated record set. Individuals have access to inspect and obtain copies of protected health information about individuals in the designated record set.  
  
Individuals have access rights to the data for as long as the health care provider retains the data after the account is deleted.  
  
The scope of what can be Data Exported is limited and must allow access to the information defined in protected health information.

**Regulation(s) in question:**

45 CFR § 164.524 - Access of individuals to protected health information.

<https://www.law.cornell.edu/cfr/text/45/164.524>

**Recommendation:**

* Specify that we will continue to retain your medical data when your account is deleted, that you have the right to have the data disclosed, and the procedures for disclosure.
* Specify the content of protected health information in the data to which you have access and provide an accessible interface.