Milestone 3

CareAway Treatment Planner

**Date**: 12/7/2017

**Team Name**: Team Tangent

Eugene Mesina (014455816) Meeting Manager (Team Leader)

Felix Huang (013427386) Documentation Manager

Jimmy Chao (012677182) Accountability Manager

Taylor Tobin (011871260) Technology/Information Manager

Crystal Chun (012680952) Quality Manager

Tyler Dao (013343302) HIPAA Manager

**Table of Contents**

[**Version Control**](#_sqxt9das6a13) **3**

[**Introduction**](#_k4j3rcunmf6s) **4**

[Abstract](#_32ocmt29l9l8) 4

[Document Overview](#_eebi1egcxx2z) 4

[Scope](#_6pidroq3kyo7) 4

[**Positioning**](#_tu66gpp3akiz) **8**

[Problem Statement](#_b7kwihrxct50) 8

[Business Opportunity](#_x0xy49eby42r) 8

[Product Position Statement](#_tcg6gsi6ewam) 9

[User Incentive](#_a5iop1hs9dfy) 10

[**Market Demographics**](#_5l1z7zxmv9ox) **11**

[Stakeholders](#_ygx5vmkj6uab) 11

[Competition](#_tdy4wq5tlee5) 11

[CHOC Link](#_tyiq54dbo813) 11

[WebPT](#_tnoplcrmwaub) 12

[**Key Assumptions and Constraints**](#_96ja5i5yf6ds) **13**

[Assumptions](#_j7egsurvlanx) 13

[Constraints](#_qv0gbnuzj8r) 13

[PHI and HIPAA Overview](#_bvg3nqe67buw) 13

[Who Must Adhere to HIPAA](#_31uqx4jgsq3a) 14

[HIPAA Privacy Rule](#_2punij80cl3r) 14

[HIPAA Security Rule](#_70norwj7dwiu) 15

[Resolution](#_psd5prjkcb4n) 16

[References](#_cjh9bo1auiyr) 17

[**Business Requirements**](#_haowq61ycdvb) **18**

[Use Case Matrix](#_luk3c7gq0oz4) 18

[Requirements](#_8p54jhqjwatv) 19

[Registration](#_cpev7ouajknw) 19

[Authentication/Session Termination](#_a876t0w57rd7) 24

[Data Access](#_ou9bvail50lf) 28

[Error Handling](#_8g4z8r4203xq) 30

[User Management](#_fu4f9jd8cl42) 32

[User Access Control](#_5n6f0089cjo4) 34

[Network Connectivity](#_iyq01zi2gb2h) 36

[Security](#_gryqwzf270ax) 38

[Treatment Plan Creation and Revision](#_muhdged16mna) 40

[Treatment Plan Interaction](#_dh9xmgav38dh) 42

[Appointment Scheduling](#_qllxnohl9fz6) 44

[Data Analysis Report](#_h9bwqav2u6qq) 47

[**Glossary**](#_diofrht5w0jh) **48**

# **Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Revision Date** | **Members** | **Description** |
| 1 | 10/5/2017 | Jimmy, Felix, Crystal, Eugene | Initial Draft. |
| 2 | 10/15/2017 | Jimmy, Felix | Scope was redefined. ICD-10 codes have been defined for the 6 common disorders listed. |
| 3 | 10/22/2017 | Jimmy, Felix, Crystal, Tyler | Scope was redefined again. Use Case Matrix, HIPAA Resolution, Business Requirements were updated to fit the new scope.   Peer-to-Peer Communication, Tutorials, and Data Analysis Reports functionalities were removed. |
| 4 | 11/10/2017 | Eugene, Felix | Scope and business requirements are changed to reflect changes discussed with our client during the 10/31 Stand-Up Meeting. Data Analysis Reports was added back into the project as requested by the client. |
| 5 | 11/18/2017 | Felix | Workflow diagrams are updated to reflect revised scope and business requirements. Glossary has been slimmed down to remove superfluous terms. |
| 6 | 11/25/2017 | Felix | Minor changes made to business requirements to make sure they are in line with workflow diagrams |

# **Introduction**

## Abstract

CareAway Treatment Planner is a web application that addresses communication issues between the patient and medical professional outside of the medical environment. As a solution that exists in the healthcare domain, it is important for CareAway to adhere to Health Insurance Portability and Accountability Act (HIPAA) standards in terms of privacy and data security. The target population for the CareAway system is patients who have a diagnosis and the medical professionals who will be overseeing their care. One goal of this system is to ensure convenience and accessibility for the user. The system can be accessed from anywhere and at anytime, as long as the user has valid login credentials. The difference between CareAway and other existing solutions is that the former will offer better means for communication between patients and medical professionals through interactive treatment plans.

## Document Overview

The purpose of this document is to define and analyze the features of the CareAway Treatment Planner. It focuses on the stakeholders and target users for the application and how the application will address one or more needs for these individuals. These needs will be represented further in the *Problem Statement* and *Business Opportunity* sections below. All business requirements for the system must be reflected in a version of this document in order to be incorporated into the final implementation. This document also details the functional and nonfunctional requirements of the system. Any words or phrases specific to the CareAway Treatment Planner are defined in the *Glossary* section of this document.

## Scope

This document applies to the CareAway Treatment Planner, which will be developed by the members of Team Tangent. The CareAway Treatment Planner will be a single page web application. CareAway will be developed to be accessible on desktop web browsers while adhering to HIPAA Standards.

In the minimum viable product, the CareAway Treatment Planner will be supported on the following desktop browsers:

Google Chrome v62.0.3202.94 (2017-10-15) or newer

Mozilla Firefox v57.0 (2017-11-14) or newer

Apple Safari v11.0.1 (2017-10-31) or newer

The target market segment for this solution includes medical professionals (including but not limited to physicians, therapist, family practitioners, and psychiatrists) along with their patients living in the United States. The CareAway Treatment Planner is meant to be used in a hospital or medical facility environment for medical professionals and at any location that can provide access to the system for the patient. The role of the system administrator will be to notify users of a breach after it has occurred.

A *medical professional* will be defined as an individual who provides health care and advice in a systematic way to people who have a medical diagnosis or condition.

A *patient* will be defined as an individual who is scheduled to receive treatment from the medical professional.

The *system administrator* will be defined as an IT professional who works for the CareAway team. The role of the system administrator will be to notify users of a breach after it has occurred.

In the minimum viable product, the CareAway Treatment Planner will support up to 150 users - a combination of a single system administrator, any number of medical professionals, and patients - as a baseline. This number will increase as future versions of the software are refined and released. In this system, a medical professional can have multiple patients that they are overseeing at one time, but a patient can only register under a single medical professional.

This system will be developed for use in the contiguous United States and is intended for an audience who speaks and reads English. To be compliant for use in the U.S. medical setting, CareAway will also adhere to HIPAA standards. Using this system will require access to the Internet, a functioning computer and monitor, and a QWERTY keyboard. Finally, to avoid any legal ramifications, use of the CareAway Treatment Planner will be limited to adults, individuals who are at least 18 years of age.

In America, three common physical disorders are diabetes, asthma, and high blood pressure, and three common mental disorders are Generalized Anxiety Disorder, Panic Disorder, and Social Anxiety Disorder. Below is a short description of these six disorders and the three most common treatment activities associated with each one.

1. Diabetes (ICD-10 Code E10 and E11)

Definition: a condition where an individual experiences high glucose levels due to little or no insulin being produced by their pancreas.

* 1. Checking your blood sugar - An individual checks their blood sugar with a glucometer. They do this to ensure their blood sugar does not go too high or fall below a specific range. In the early stages of treatment after diagnosis, the individual usually reports blood sugar levels to their doctor.
  2. Aerobic exercise - Also known as cardio, this type of exercise requires the heart to pump oxygenated blood to working muscles. Essentially, the individual performs some exercise to get their heart pumping. 30 minutes of aerobic exercise is recommended. Aerobic exercise includes but is not limited to running, walking, and swimming.
  3. Strength training - This type of exercise requires an individual to lift a set of weights. The size of those weights will usually be in the 10 - 20 pound range. It is recommended to do strength training 20 - 30 minutes about 3 times a week.

1. Asthma (ICD-10 Code J45)

Definition: a condition where an individual experiences muscles around the airways tightening, causing coughing, wheezing, and shortness of breath during periods of movement.

* 1. Taking corticosteroids - Corticosteroids are a type of medication that open up airways and relieve inflammation.
  2. Using a peak flow meter - A peak flow meter is a device used to measure how well air moves out of an individual’s lungs. Individuals use this device by blowing into it, and it provides them a reading of their peak expiratory flow (PEF).
  3. Using nebulizers - A nebulizer is a machine that converts liquid medication into a mist that the individual inhales. A nebulizer treatment lasts between 5 - 15 minutes.

1. High Blood Pressure (ICD-10 Code R03.0)

Definition: a condition where the force of blood against the arteries is too high.

* 1. Monitoring Blood Pressure with a Blood Pressure monitor - an individual can easily use a blood pressure monitor to check their blood pressure and report it to their doctor.
  2. Aerobic exercise - Also known as cardio, this type of exercise requires the heart to pump oxygenated blood to working muscles. Essentially, the individual performs some exercise to get their heart pumping. 30 minutes of aerobic exercise is recommended. Aerobic exercise includes but is not limited to running, walking, and swimming.
  3. Medication - Take Beta blockers or ACE inhibitors.

1. Generalized Anxiety Disorder (ICD-10 Code F41.1)

Definition: a condition where an individual’s severe anxiety interferes with their daily activities.

* 1. Supportive-expressive therapy - Patient can focus on anxiety as an outgrowth of feelings about relationships. Patient talks about their disorder and talks about how it affects them and those around them.
  2. Cognitive behavioral therapy - Patient learns and practices behavioral relaxation techniques as well as restructuring.
  3. Relaxation Visualization - A therapist suggest relaxing images, pleasant smells, and sounds for patient to think about.

1. Panic Disorder (ICD-10 Code F41.0)

Definition: an anxiety disorder where the individual experiences recurrent panic attacks.

* 1. Talk therapy - Patient communicates with therapist; sit down and understand what panic disorder is.
  2. Counseling - Patient works with patient’s symptoms until it becomes less terrifying to the patient.
  3. Relaxation - Patient learns relaxation and breathing techniques to make panic attacks less severe and easier to cope with.

1. Social Anxiety Disorder (ICD-10 Code F40.10)

Definition: A chronic condition where an individual experiences anxiety while socializing.

* 1. Exposure therapy - Patient faces their fear slowly until they do not fear it anymore. This may include going out to public, public speaking.
  2. Social skills training - Patient develop social skills through rehearsing or role-playing. This helps the patient become more comfortable with real social situations.
  3. Cognitive restructuring - Patient learns to identify fear and takes steps to overcome it.

The minimum viable product will be able to support *actionable tasks* for the treatments of each of the six common disorders. An *actionable task* is a piece of work determined by the medical professional that the patient can perform on their own.

# **Positioning**

## Problem Statement

In the current medical treatment environment, a patient’s relationship with their medical professional is usually paused as soon as the patient walks out of their medical professional’s facility. During the time of the visit, the patient may receive a diagnosis, some prescriptions, and a set of instructions from their medical professional to go about treatment. However, that’s usually where the care stops. The only time that relationship resumes again is when the patient has another in-office appointment to see the medical professional.

If the patient has never been diagnosed with their current condition before, all they will know about it will be confined to the discussion they had with their medical professional along with the prescriptions and other written instructions that were provided to them. What is the patient to do if they have a question on how to take a certain medication, or if their condition worsens? What if the patient is unsure of if they are following their treatment plan correctly? These questions could only be answered if the patient comes in again for another appointment. However, appointments are very timely and sometimes inconvenient for the patient. They have to schedule an appointment and make time during the day for it. In the event that the patient’s condition is a physical ailment, commuting to the medical professional’s facility becomes even more of a hassle and can sometimes be a liability.

From the medical professional’s point of view, their knowledge regarding the patient and their condition is limited to any reports that were generated during the time of the appointment. There is no way for the medical professional to ensure that the patient is improving on a day-to-day basis or going about their treatment correctly. Furthermore, the medical professional is unable to directly reach out to their patient if a better treatment plan becomes available.

## Business Opportunity

In the previous section, *Problem Statement*, multiple flaws were identified regarding the current medical treatment environment.

Here are flaws that were identified for patients:

* Difficulty in managing their diagnosis, especially if the diagnosis is long-term or new
* Difficulty in understanding treatment for their diagnosis
* Limited access to professional advice outside of scheduling an appointment
* Lengthy time commitments due to scheduled appointments
* The need to travel with an impairment

Here are the flaws that were identified for medical professionals:

* Lack of communication with the patient after an appointment
* Difficulty in understanding the effectiveness of the treatment plan
* Inability to revise the treatment plan if current methodologies are ineffective

Given these flaws, a system needs to be put in place that addresses this set of problems in their entirety. There currently isn’t a product on the current market that does so. Systems have been implemented in medical facilities to record patient data, but they are intended for medical professionals only. They are not designed to share information or to be accessible to the patient. Patients have access to reminder and to-do list applications that are available to download, but they are not designed to be used for medical treatment and provide no quick way for the patient to seek medical advice.

## Product Position Statement

CareAway Treatment Planner is an online single page web application that will function as a medical care oversight and scheduling system. CareAway allows medical professionals to create online treatment plans which will be accessible by the patient in the comfort of their own homes or wherever they choose to access the system. The goal of this system will be to provide a solution to address the flaws in the current medical treatment environment.

The CareAway Treatment Planner is aimed towards this target market to provide an ease of service and bridge the gap between medical professionals and patients outside the medical facility. There are currently around 12 million medical professionals in the United States (results from Kaiser Family Foundation) and a never-ending number of patients who are receiving treatment for some type of medical need. The CareAway Treatment Planner assists our target market segment by improving a medical professional’s interaction and connection to their patients. In addition, it will also provide ease of access to patients by allowing them to keep track of their treatment plan and provide feedback if necessary. There is a growing need for this solution in the healthcare industry and CareAway aims to address the needs to medical professionals and patients.

The key issue that the CareAway Treatment Planner addresses will be maintaining the connection between medical professionals and their patients after their appointment. As mentioned in the section *Problem Statement*, the relationship between patient and medical professional is paused when the appointment concludes. CareAway addresses this problem by allowing a means of interaction between the two parties after the patient leaves the medical facility.

On the CareAway Treatment Planner, the medical professional creates a treatment plan with actionable tasks for their patient. When the patient accesses the system, they will see day-to-day instructions for their treatment detailed out by the medical professional. As the patient goes through these instructions each day, they are able to report that they have completed each task and send feedback regarding any pain or ineffectiveness that they notice with the current treatment plan. On the medical professional’s account, they are able to monitor the patient’s progress with the current treatment and can revise the treatment plan on the fly if the current plan is not suitable.

The CareAway Treatment Planner will allow significant improvement in the convenience and accessibility of a treatment plan. The patient will be able to view and follow the treatment plan at their convenience. This reduces the need for the patient to make scheduled in-office appointments and in turn, they will not be inconvenienced to go back and forth between their home and the medical care facility. The medical professional will have an easy and effective way of monitoring their patient. They will be able to track the patient’s day-to-day progress and ensure that the patient is following the treatment plan. This will allow the medical professional to provide a treatment plan suited to their patient’s specific condition and make changes to it if necessary.

## User Incentive

As mentioned in the previous section, the CareAway Treatment Planner will address the needs identified in the *Problem Statement* and *Business Opportunity* section. This web application will benefit both medical professionals and patients. A patient will want to use CareAway because it is a platform that will help improve personal health. If the patient chooses to not use this system, they may not improve and may possibly accentuate their condition. If this happens, the patient will have to continue scheduling appointments to see their medical professional, which will cost the patient both time and money. A medical professional will want to use CareAway because they will be able to serve their patients better. Encouraging patients to use CareAway will allow the medical professional to be more active in the patient’s care and they will be able to help them heal more effectively. Because patients will be providing feedback about the current treatment plan, the medical professional can easily gain insight on their patient and quickly make suggestions to revise the treatment plan.

# **Market Demographics**

## Stakeholders

|  |  |
| --- | --- |
| Stakeholders | Roles |
| Medical Professionals | The Medical Professional will be a user of the system and use it in the context of their practice to provide care in the form of actionable tasks to the Patient. |
| Patients | The Patient will use the system during their treatment to follow the treatment plans created by the Medical Professional. |
| System Administrators | The System Administrator will notify users of a breach after it has occurred. |
| Software Developers | The Software Developer will perform the design and documentation for the system. They will implement the system using software and debug code if needed. |
| Q/A Testers | The Q/A Tester will use the system and put it through its paces. The will report on any found bugs to the Software Developer. |

## **Competition**

### CHOC Link

CHOC Link is a web application used by Children’s Hospital of Orange County (CHOC). This system is free of charge to use for patients or parents of patients. During the time of a patient’s appointment, the doctor enrolls the patient into the CHOC Link system using only the patient’s email. The patient will then receive an email invitation to sign up for the system and follows instructions included in the email to set up their account. Once the patient’s account is set up, the doctor is able to upload the patient’s lab results and prescriptions from their most recent appointment. The doctor can also write a Discharge Document, a high level recap of the appointment which includes data such as the patient diagnosis and treatment suggestions. Some of the services that CHOC Link provides for the patient are messaging doctors and healthcare teams, requesting and changing an appointment, viewing current prescriptions, and paying bills.

CHOC Link is the closest competitor to the CareAway Treatment Planner in terms of functionality. CHOC Link is not adequate for a doctor to monitor a patient to see if they are improving on a day-to-day basis. CareAway Treatment Planner offers tools for doctors such as creating and altering a patient’s treatment plan, seeing their daily progress, and receiving feedback from patients.

Reference: <https://www.choc.org/choc-link/>

### WebPT

WebPT is a web application that acts as a hybrid scheduling system and patient management system for physical therapists. This system has a calendar-like interface to easily view and edit schedules for patients and physical therapists at the treatment location. The physical therapist also has the option to set recurring patient appointments using drag and drop functionality. The physical therapist also has the option to search for their patients to upload documents and patient records.

The drawback with this system is that it is tailored towards the physical therapy field. The CareAway Treatment Planner will be able to handle the needs of patients with the 3 most common physical and mental disorders. The medical professional will be unsure of the patient’s well-being until the next appointment. On CareAway, the medical professional will be able to track the patient’s day-to-day progress.

References: <https://www.webpt.com/products/scheduling>

# **Key Assumptions and Constraints**

## Assumptions

|  |  |
| --- | --- |
| **#** | **Assumptions** |
| **1** | **The patient, medical professional, and system administrator have readily available Internet service.** |
| **2** | **The medical professional will be able to devote time during their day to the system. They will view patient treatment plans and revise treatment plans if necessary.** |
| **3** | **The patient will be able to devote time during their day to utilize the system and follow through on the treatment plan.** |
| **4** | **Medical professional and patient have a means of communication ( ie. email, phone, or text.)** |

## 

## Constraints

### PHI and HIPAA Overview

In 1996, the Health Insurance Portability and Accountability Act was passed to improve the efficiency and effectiveness of the healthcare system in handling patients' PHI. *PHI* stands for protected health information and refers to the personal information about an individual’s health status, health care, and payment for health care. The HIPAA (Health Insurance Portability and Accountability Act) was enacted to provide data privacy and security provisions to ensure the safeguarding of medical information by *covered entities*, individuals or organizations that have access to a person’s PHI. Congress incorporated into HIPAA provisions that mandated the adoption of privacy protections for patient health information. Two of these provisions were the Privacy Rule and the Security Rule.

The HIPAA Privacy Rule provides federal protection for PHI held by covered entities and gives patients an array of rights with respect to that information. The Privacy Rule is also balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. At the same time, Congress recognized advances in electronic technology could erode the privacy of health information which led to the creation of the Security Rule. The HIPAA Security Rule sets national standards to protect individuals’ electronic personal health information that is created, received, used or maintained by a covered entity. The HIPAA Privacy Rule and Security Rule will be discussed in the subsequent sections.

#### 

#### Who Must Adhere to HIPAA

*Health Plans* - health insurance companies, health maintenance organizations (HMOs), company health plans, and government programs that pay for health care.

*Health Care Providers* - providers that conduct certain business electronically, such as electronically storing data or billing health insurance. This includes and is not limited to doctors, clinics, hospitals, psychologist, chiropractors, nursing homes, pharmacies and dentists.

*Health Care Clearinghouses* - parties that process nonstandard health information they receive from another entity into a standard electronic format or data content, or vice versa.

*Business Associates* - The term “business associate” refers to a person or organization who is not a direct employee of a covered entity that performs certain functions and activities on behalf of a covered entity that involve the use of individually identifiable health information. Business associate functions include and are not limited to claims processing, data analysis, utilization review, and billing.

#### HIPAA Privacy Rule

The goal of the Privacy Rule is to ensure that an individual’s health information is properly protected while allowing the flow of information needed to provide and promote high quality care. The Privacy Rule permits important uses of information sharing, usually for the individual’s treatment, while protecting their privacy while they are actively seeking care.

The Privacy Rule protects all individually identifiable health information, held or transmitted by a covered entity or its business associates in any form or media, whether electronic, paper, or oral. A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual’s protected health information may be used or disclosed by covered entities. A covered entity may use and disclose protected health information only when (1) healthcare professional(s) who are overseeing a patient’s care are required to interact with PHI to perform health transactions (2) the patient that the PHI refers to provides authorization in writing. Any piece of information that can associate a person with their health information must be protected from being exposed to actors that are not crucial for healthcare transactions. These outside actors can only legally have access to the patient’s PHI if and only if the patient provides written authorization.

Conditions in which the Privacy Rule permits sharing health information are detailed below.

*To the Individual* - A covered entity is allowed to disclose protected health information to the individual

who is the subject of the information.

*Treatment, Payment, Health Care Operations* - Treatment is defined as the provision, coordination, or

management of health care and related services for an individual by one or more health care providers.

Payment is defined as the activities of a health care provider to obtain payment or be reimbursed for the

provision of health care to an individual. Health Care Operations is defined as any tasks or activities

attributed to performing health care such as quality assessment, insurance functions, and business

management activities.

*Uses and Disclosures with Opportunity to Agree or Object* - Informal permission to share information can be obtained by asking the individual outright, or by situations that clearly give the individual the

opportunity to agree or object to sharing.

*Incidental Use and Disclosure* - Incidental disclosure occurs when a bystander or outsider unwillingly or unknowingly hears or comes across the subject’s information. Not every risk of an incidental use or disclosure needs to be eliminated, as that is next to impossible. However, the covered entity is required to have reasonable safeguards set in place to minimize any incidental disclosure.

#### HIPAA Security Rule

The goal of the Security Rule is to protect the privacy of individuals’ health information while allowing covered entities to adopt new technologies to improve the quality and effectiveness of patient care. As new technologies are created, the health industry has begun to move away from paper processes and rely more on electronic information systems to handle patient information. Today, many providers use computerized physician order entry (CPOE) and electronic health records (EHR) systems. The Security Rule was passed to ensure that systems that handle CPOE and EHR have standards set in place in regards to data management and storage.

The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule also refers to this information as electronic protected health information (e-PHI). Furthermore, in compliance with the Privacy Rule, all data that exists electronically needs the individual’s written authorization before it can be shared.

The Security Rule also requires covered entities to maintain administrative, technical, and physical safeguards to protecting e-PHI.

Administrative Safeguards include and are not limited to:

* Security Management Process: Implementing security measures that reduce risks and vulnerabilities to e-PHI.
* Information Access Management: Policies and procedures to accessing e-PHI need to be

established.

Physical Safeguards include and are not limited to:

* Workstation and Device Security: Workstation devices and electronic media must be used for

their intended purpose. The covered entity must also have in place policies regarding the transfer, removal, disposal, and reuse of a workstation device or electronic media.

Technical Safeguards include and are not limited to:

* Access Control: Only authorized persons can have access to a subject’s e-PHI.
* Integrity Controls: Policies and procedures need to be established to ensure e-PHI is not improperly altered or destroyed.
* Transmission Security: Security measures must be established to guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

#### Resolution

Based on how the medical treatment environment is structured, all U.S. patients receiving medical care are protected under HIPAA. This means that they are legally entitled to the privacy of all PHI relating to them, regardless of if it exists on traditional media (papers, physical lab reports) or in electronic form. Given that the CareAway Treatment Planner will be handling PHI, it will be important for the system to adhere to HIPAA protocol.

To address technical safeguards in the Security Rule, CareAway will be developed using a HIPAA compliant web service to ensure security and privacy in data storage and accessibility.

In adherence with the HIPAA Breach Notification Rule, a designated individual will act as the system administrator for this system. Their role, as mentioned in the *Scope* section, will be to notify all medical professionals and patients using the CareAway Treatment Planner of breaches after they have occurred. In the event that a breach does occur, the system will display a message to all users.

Authentication and access control will be addressed by ensuring that all users are using a valid username and password to login to the system. In the event that any user does not type a valid username or password, then the system will not allow them to proceed and display a message that they have entered invalid credentials and should try again, until valid credentials are entered.

During the patient’s registration, the CareAway Treatment Planner will require written authorization from patients looking to utilize the service. This authorization will require the patient to acknowledge that all or part of their PHI will be online. By doing this, the CareAway system is complying with HIPAA privacy standards by obtaining the patient’s acknowledgement and authorization. To protect incidental disclosure, the patient will enter in a unique medical professional registration identifier during their registration. This will tie the patient to that medical professional and will give the medical professional that the registration identifier corresponds to access to viewing and changing the patient’s PHI.

In the event that a breach has occurred, the system will display a message to the users informing them of the breach and that measures are being taken to secure the system.

#### References

References for the above information can be found in the links provided below.

<https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html>

<https://www.hhs.gov/hipaa/for-professionals/index.html>

<https://www.hhs.gov/answers/hipaa/what-is-phi/index.html>

<http://www.bostonscientific.com/en-US/corporate-citizenship/compliance-ethics/patient-privacy-hipaa.html>

<http://www.molinahealthcare.com/providers/ut/medicaid/manual/PDF/Section_16_HIPAA.pdf>

# **Business Requirements**

## **Use Case Matrix**

## 

## 

## 

## Requirements

### **Registration**

**Business Requirement**: User needs a way to create an account to gain access to the system

Actors: Medical Professionals, Patients

Precondition:

User must have a functioning Internet connection.

Functional Requirements and Criteria:

Functional: The system will have a way to differentiate between patient and medical professional registration.

The user has a way to set up their account.

* The user is directed to register themselves on the CareAway Treatment Planner.
* A user can register as a patient or a medical professional.

The user will need to provide a first name during their account creation. Criteria for a first name will be as follows:

* 1 - 30 characters [A-Z or a - z and any special characters ]
* **Business Rule:** *Special characters* will be defined as any non-alphanumeric keys that are found on a standard 87 key QWERTY keyboard.

The user will need to provide a last name during their account creation. Criteria for a last name will be as follows:

* 1 - 30 characters [A-Z or a - z and any special characters ]
* **Business Rule:** *Special characters* will be defined as any non-alphanumeric keys that are found on a standard 87 key QWERTY keyboard.

The user will need to provide a valid username during their account creation. Criteria for a username will be as follows:

* Must be unique. Cannot be an already existing identifier
* 8 - 120 characters [A - Z or a - z]
* Must contain at least 1 numeric digit [0-9]
* No special characters with the exception of the @ symbol and . symbol
* No spaces

The user will need to provide a valid password for their account. Criteria for a password will be as follows:

* + 8 - 120 characters [A - Z or a-z]
  + Must contain at least 1 numeric digit [0 - 9]
  + Special characters allowed: ! @ # $ % &
  + Cannot be solely numbers or solely letters
  + No spaces
* Password criteria will show during registration

The medical professional and patient will have a way to associate with one another.

* **Business Rule:** The medical professional will have a unique identifier that the patient will need to enter during their registration.

The user must provide an answer to 3 security question that the system provides to them.

* **Business Rule:** These are the security questions the system will provide. Security questions will be divided into 3 non-intersecting sets of questions, where the user can choose 1 question from each set.
* Answers to the security questions will be entered through keyboard input as text.
* Criteria for security question answers will be as follows:
  + 1 - 100 characters [ A-Z, a -z, 0 - 9]
  + Special characters and spaces will be allowed

The patient needs to provide written authorization to the system acknowledge use and sharing of health information.

The patient needs to provide written authorization to the system acknowledge that they are an adult (18 years of age or older).

The medical professional and patient can proceed through registration once they have entered the required data and the data has been validated.

Postcondition (Success): The user will be prompted that they have successfully registered and created their account.

Failure: If the user provides an invalid user input, they will be prompted that they cannot proceed in the registration process, (Ex. Input a bad username, bad password, failure to answer security questions, an invalid medical professional registration identifier, invalid first name or last name) and they will be prompted to fix the error. They will not be allowed to proceed with registration.

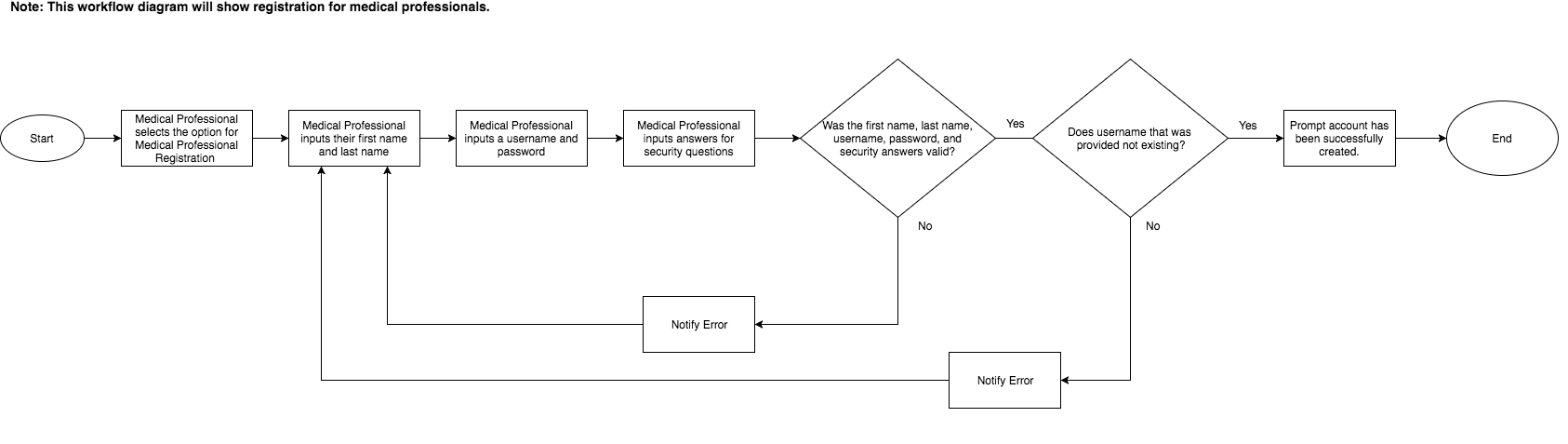
If the user provides an already existing username, they will be prompted that the username already exists and they must choose another username. They will not be allowed to proceed with registration.

If the system fails to write valid user input to the database, prompt the user that an error occurred and the user should try registering again.

If the system fails to recognize the request, the system will prompt the user that it has failed to handle request and that they system is currently unavailable.

If the patient does not agree to provide written authorization, they will be prompted that authorization must be provided in order to utilize the service.

If the patient does not provide a valid medical professional identifier, they will be prompted that they will need to provide a valid input here. They will not be allowed to proceed with registration.



### 

### 

### 

### 

### **Authentication/Session Termination**

**Business Requirement**: A user needs a way to access the system to start their activities and end their user session once they want to end their activities on the system.

Actors: Medical Professionals, Patients, System Administrators

Precondition: A user must be registered into the system. The user must be logged in and must have an Internet connection. The user must be at the appropriate page for logging in, logging out, or resetting their credentials.

User Story: As a user, I want to log in to the system to access my data and log out so that I can end my current session and others will not be able to see my account.

As a user, I want to reset my credentials so that I can access the system, when I do not remember my password.

Functional Requirement(s) and Criteria:

User is able to enter in username into username field.

* User enters in their their unique username they chose during registration.

User is able to enter in password into password field.

* Password must be the one that corresponds to the user’s account username.
* Password should not be visible as plain text. Each character the user types should not be human readable after the key has been pressed.

User has a way to proceed after they have typed in their credentials

* User is redirected to their account within 3 seconds of their submission.

User can request to reset their credentials

User must verify who they are when they choose to reset their credentials.

* **Business Rule:** User must first provide their user name
* **Business Rule:** System retrieves the 3 security questions that the user answered during registration.
* The user must answer the 3 security questions exactly as they did during user registration.

User is prompted to provide new valid password when resetting their credentials.

* Criteria for a password will be as follows:
* 8 - 120 characters [A - Z or a-z]
* Must contain at least 1 numeric digit [0 - 9]
* Special characters allowed: ! @ # $ % &
* Cannot be solely numbers or letters

The system will ensure the user has input the desired password when resetting their credentials.

* **Business Rule:** The user will have to type their desired password 1 more time.
* The user must input the same password they previously provided.

User can terminate their user session

User is prompted they have ended their session

Session automatically times out

* After 15 minutes of session inactivity, a message will appear prompting the user if they are still active on the current session.
* **Business Rule:** *Session inactivity* will be defined as no input on the page
* If the user remains inactive 2 minutes after the message has appeared, their session will be automatically terminated.

Postcondition (Success) : If the user is logging in and they provided valid credentials, they will be directed to their account. If the user is trying to logout, user session will be terminated. If the user chose to reset their credentials, the user now has a new updated password they can use to log into the system after they have properly verified themselves.

Failure:

If the user has entered an invalid username/password, then they are prompted to enter their username/password again.

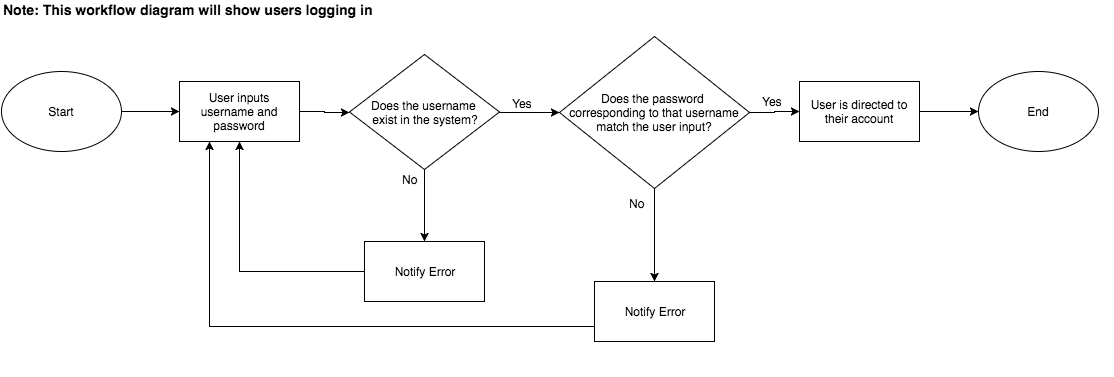
If the system fails to recognize a request, the system will prompt the user that it has failed to handle request and that they system is currently unavailable.

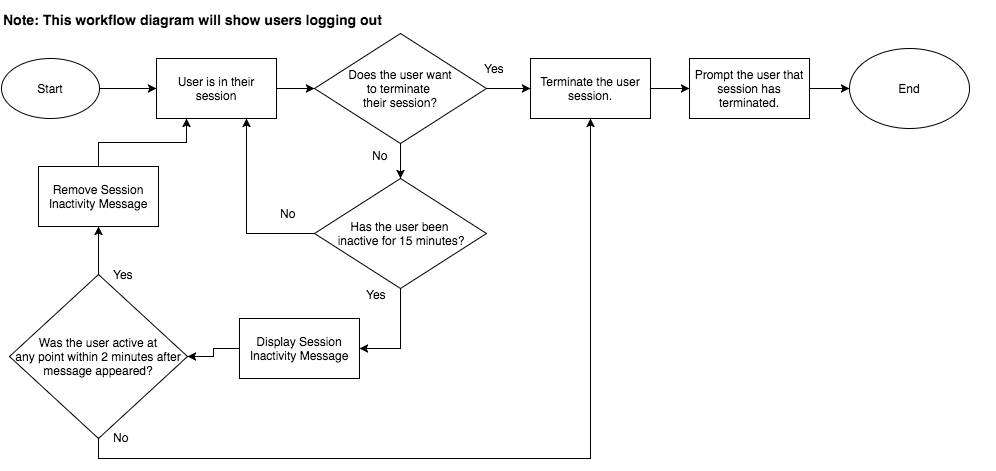
If the user inputs an invalid user name during the resetting credentials process, then the system must prompt the user they did not provide a valid user name.

If the user fails to answer any 1 of the 3 security questions correctly, the system will prompt the user that they have provided an invalid security answer.

If the user does not enter a valid password, they will be prompted that their password must match the password criteria.

If the user does not provide the same password 2 times, they will be prompted that both passwords must match.





### 

### 

### **Data Access**

**Business Requirement**: A user needs to read, edit, or delete data from the system

Actors: Medical Professional, Patients

Precondition: The system must be active and deployed.

User Story: As a user, I want to access my data in order to manipulate it.

Functional Requirement(s) and Criteria:

Medical Professionals have access to the following data:

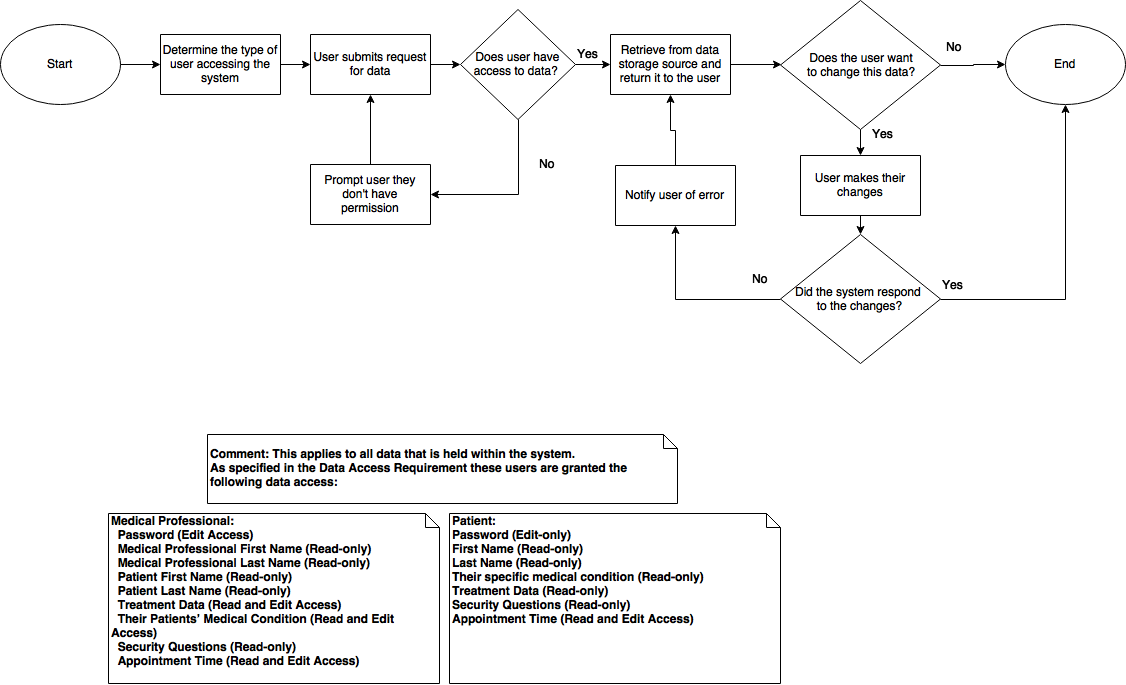
* Password (Edit Access)
* Medical Professional First Name (Read-only)
* Medical Professional Last Name (Read-only)
* Patient First Name (Read-only)
* Patient Last Name (Read-only)
* Treatment Data (Read and Edit Access)
* Their Patients’ Medical Condition (Read and Edit Access)
* Security Questions (Read-only)
* Appointment Time (Read ,Delete ,and Edit Access)

Patient have data access to the following data:

* Password (Edit-only)
* First Name (Read-only)
* Last Name (Read-only)
* Their specific medical condition (Read-only)
* Treatment Data (Read-only)
* Security Questions (Read-only)
* Appointment Time (Read, Delete, and Edit Access)

Postcondition (Success): Users have data access to their data within the system

Failure: If a user is trying to change a field and the system is not responding, then prompt them of the system error and to reload the page.



### **Error Handling**

**Business Requirement**: The system needs a way to handle potential errors either caused by the user, the system, or both.

Actors: System

Precondition: The system is active and deployed.

User Story: As a user, the system I am using must be able to identify and catch any errors that occur.

Functional Requirement(s) and Criteria:

System detects user-caused errors.

* Errors include:
  + User entering invalid data
  + User attempting to access data that they are not allowed to access
  + Users attempting to change data they are not allowed to change
  + User attempting to access system when it’s down

System detects system-caused errors.

* Errors include:
  + The system is not rendering the user interface
  + The system is not storing data properly
  + The system cannot access data that it should have access to

System handles all potential errors.

* Handling methods include:
  + Alerts to the user if they caused an error
  + Alerts to the user if the system does something unexpected
  + Automatically reverting any changes that caused the error

Postcondition (Success): Error is handled by the system. In certain cases, the user will be notified of errors.

Failure:

If the system fails to handle an error properly, the system will have to be fixed. The CareAway team will have to intervene to solve the issue.



### **User Management**

**Business Requirement**: The system needs a way to create, read, and update its users.

Actors: System

Precondition: The system is active and deployed.

User Story: As a user, I want the system to be able to manage my account and relating data.

Functional Requirement(s) and Criteria:

The system allows the creation of new user accounts.

* Creation is done through a user registering into the system.
* The system will store the new user after the user is created.

The system can access all of its user's account credentials.

* System reads user data in order to validate them.

The system can update its users.

* System can access active user accounts to modify their information.
* Credentials will persist unless changes are made.

**Business Rule:** In the event changes are made, they must be stored

The system can change users’ state by creating their session and/or terminating their session.

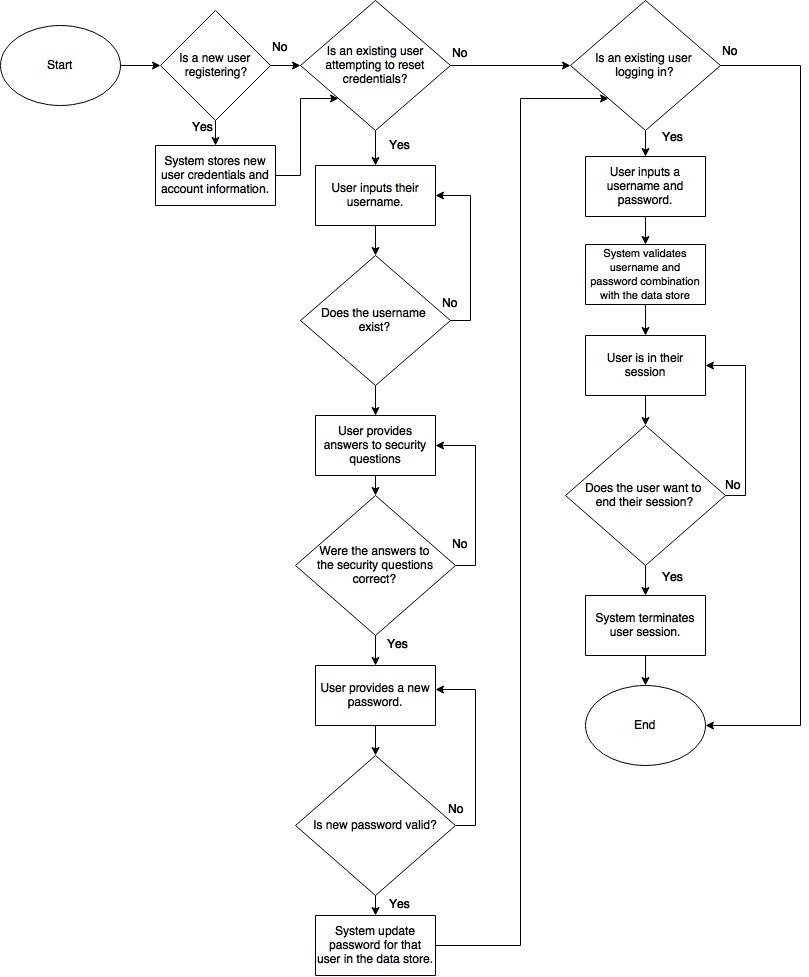
* System provides user a way to log in
* System provides user a way to log out

Postcondition (Success): The system is able to create new users, view all of its users’ credentials, and modify existing users’ credentials.

Failure:

If the system tries to change the user’s credentials and the change does not persist, then the system should alert the patient that their credential change was not saved and that the patient should reload and try again.

If the system cannot access active user accounts, then the system will not be available for use and needs to go under maintenance and the CareAway team will need to take action.



### **User Access Control**

**Business Requirement**: The system needs to be able to control access to what users can see and interact with.

Actors: Patient, Medical Professionals, System Administrators

Precondition: The user must be registered with the system and have login credentials. The user must have Internet connection.

User Story: As a user, I want to ensure that after I login to the system, I can see data relating to me specifically and manipulate it.

Functional Requirement(s) and Criteria:

The medical professional will have medical professional access control, access to the options and functionalities that are meant for him/her.

* Medical professional has access to their patients’ data.
* Medical professional can view and edit their own account data.
* Medical professional has access to their own appointments.
* Medical professional is able to create and revise treatment plans and request an appointment with their patient.

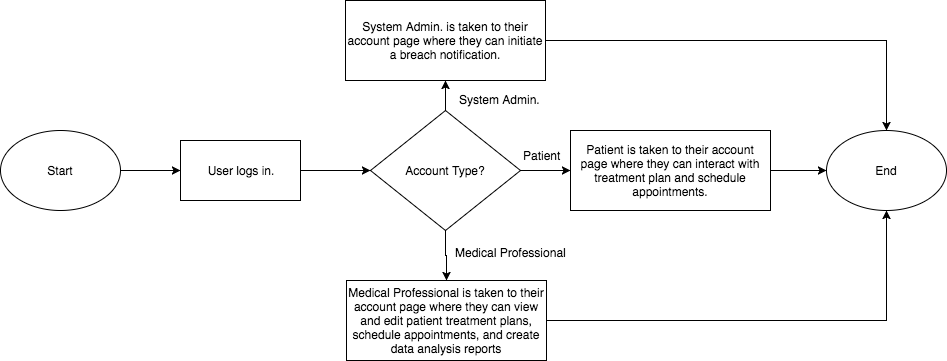
The patient will have patient access control, access to options and functionalities that are meant for him/her.

* Patient can view and edit their own account data.
* Patient has access to their own medical data (treatment plan).
* Patient can access their treatment and request an appointment.

The system administrator will have system administrator access control, access to options and functionalities that are meant for him/her.

* System administrator can send breach notifications.

Postcondition (Success): The user has access to what is meant for them, specifically.



### 

### **Network Connectivity**

**Business Requirement:** The system needs to be able to connect to third-party technology.

Actors: System

Precondition: The system is deployed and active.

User Story: The system needs a way to connect to different services.

Functional Requirement(s) and Criteria:

System connects to third-party Infrastructure as a Service (IaaS).

* Systems utilizes Infrastructure for deployment.
* System is able to persist on Infrastructure.
* System connectivity is able to persist.

System can communicate with third-party Software as Services (SaaS).

* System sends data to the third-party technology.
* System gets data back from the third-party technology.

Postcondition (Success):

The system can connect to the third-party technology and communicate with it.

Failure:

If the system cannot send or get data to/from the third-party technology, then the areas of the web application using the data will be empty.

If the system cannot connect to the third-party technology, then the areas of the web application using the data will be empty.

### 

### 

### 

### 

### **Security**

**Business Requirement:** The system has a way to ensure secure connections and notify users of security vulnerabilities.

Actors: System Administrator, System

Precondition: System is deployed and running on the world wide web.

User Story: As a user, I want a secure way to connect to the system and be notified of any breaches within it.

Functional Requirement & Criteria:

The system ensures all connections to the server are valid.

* The system will ensure all sessions are secure until terminated.
* All access to the system, including data access and data modification, will require verification and authentication to ensure the user is valid.

A breach message will display that will notify users of a breach.

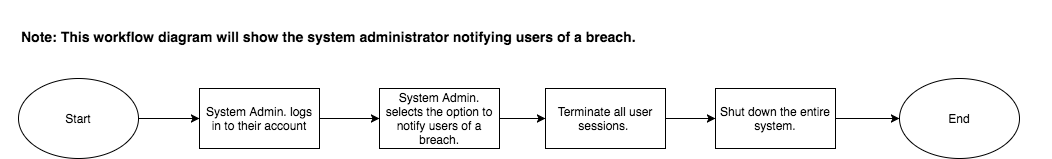
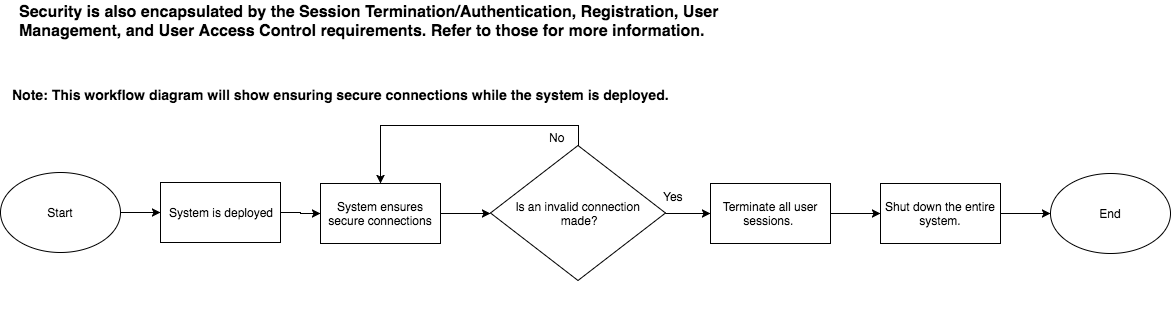
* The message will display that a breach has occurred.
* **Business Rule:** When a breach message appears, the user will no longer have access to the system.

Postcondition (Success): User can connect to the server securely.

If a breach occurs, all users are notified of the breach by the system administrator.

Failure: If the system is breached, and users are not notified of the breach, then the system will need to redirect the user to the breach message, all user sessions will be terminated, and the system will be shutdown for all users.

If any invalid connections are made to the server, terminate the session and shutdown the system for all users.



### **Treatment Plan Creation and Revision**

**Business Requirement**: The medical professional needs a way to create and revise treatment plans for a patient.

Actors: Medical Professional

Precondition: A medical professional must be registered into the system.

User Story: As a medical professional, I want to create treatment plans for a patient, in order to better their condition.

Functional Requirement(s) and Criteria:

Medical professional can select a patient they want to make a treatment plan for.

* The medical professional can only select a patient that is currently assigned to them.
* Medical professional can set the patient’s diagnosis/condition.

Medical professional can assign tasks on certain days for the patient.

* **Business Rule:** Tasks will be assigned through different types of widgets.
  + Check List Widget - list of activities added by the medical professional that can be marked as complete by a patient.
  + Meter Widget - numerical scale with a list of possible values used for reporting patient pain.

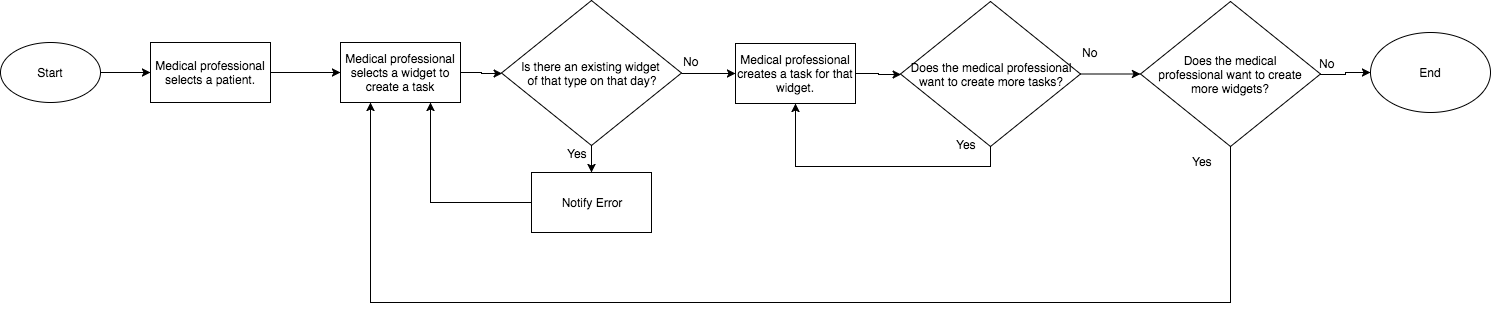
Medical professional can revise an existing treatment plan.

* The medical professional can remove individual tasks from the Checklist widget.
* The medical professional can edit and add individual tasks on the Checklist widget.
* The medical professional can delete widgets from a patient’s treatment plan entirely.

Postcondition: Treatment plan was created successfully for the patient. The medical professional was able to create and revise patient treatment plans.

Failure: If the treatment plan failed to save or be sent to the patient, the medical professional will be notified that the treatment plan failed to save.

If the medical professional attempts to add widget to a day on the patient’s treatment plan where that widget type already exists, the medical professional will be notified of this error.



### **Treatment Plan Interaction**

**Business Requirement:** The patient needs a way to use the system to perform the tasks in their treatment plan.

Actors: Patients

Precondition: The patient must must be registered in the system and be logged in. The patient must have a treatment plan that has been made for them by the medical professional.

User Story: As a patient, I want to access my treatment plan so that I can perform the activities to better my condition.

Functional Requirement(s) and Criteria:

When the patient logs in, they should see their treatment plan

* The treatment plan should display all the tasks created by their medical professional and any upcoming appointments.

Patients can interact with their treatment plan.

* Patient can only interact with the widgets on the treatment plan on the current day
* Patient has a way to tell the medical professional that they have completed a widget’s activity.
* **Business Rule:** For the meter widget, patient interaction will be handled by having them select a numerical value on that widget.

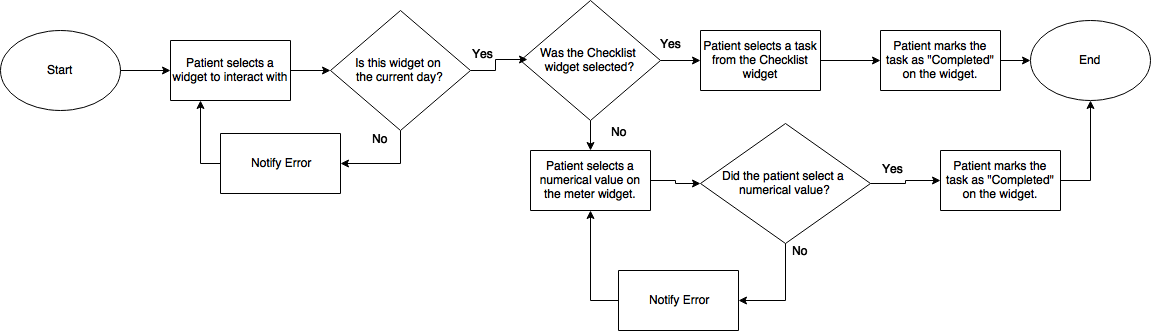
Patient has a way to differentiate between completed and uncompleted tasks.

* **Business Rule**: Tasks that are not completed will display in as “In-Progress” status and tasks that are completed will be displayed as “Completed” status.

Postcondition (Success): The patient is able to acknowledge that they have completed a task and interact with the widgets in their treatment plan.

Failure: If the patient tries to mark a task as completed that they have not previously interacted with, they will be prompted that the activity requires their interaction first.

If a patient does not perform a task on a day that has already passed, that task will not be marked as “Completed” status.



### **Appointment Scheduling**

**Business Requirement**: A medical professional and a patient need to be able to request an in-office appointment with one another.

Actors: Medical Professionals, Patients

Precondition: The user must have Internet access and be logged in to the system.

User Story: As a patient, I want to be able to coordinate appointments to receive medical care.

As a medical professional, I want to be able to coordinate appointments to provide medical care.

Functional Requirement(s) and Criteria:

Patient can request an appointment with the medical professional.

* Patient must choose a time and date that is after the current time and date.
* Patient must choose a time and date where they previously have not requested or scheduled another appointment.
* Patient must choose a time and date where the medical professional does not have an existing appointment.
* **Business Rule:** Appointments will be scheduled in 30 minute allotments.

Medical professional can request an appointment with the patient

* Medical professional must choose a time and date where they previously have not requested or scheduled another appointment.
* Medical professional must choose a time and date that is after the current time and date.
* Medical professional must choose a time and date where the patient does not have an existing appointment
* **Business Rule:** Appointments will be scheduled in 30 minute allotments.

The party that the request was sent to will be notified.

* The other party may accept or decline the appointment request.
* If the appointment was declined, then it should no longer show up for either party.
* If the appointment was accepted, then the request should show up as an official scheduled appointment for both parties.

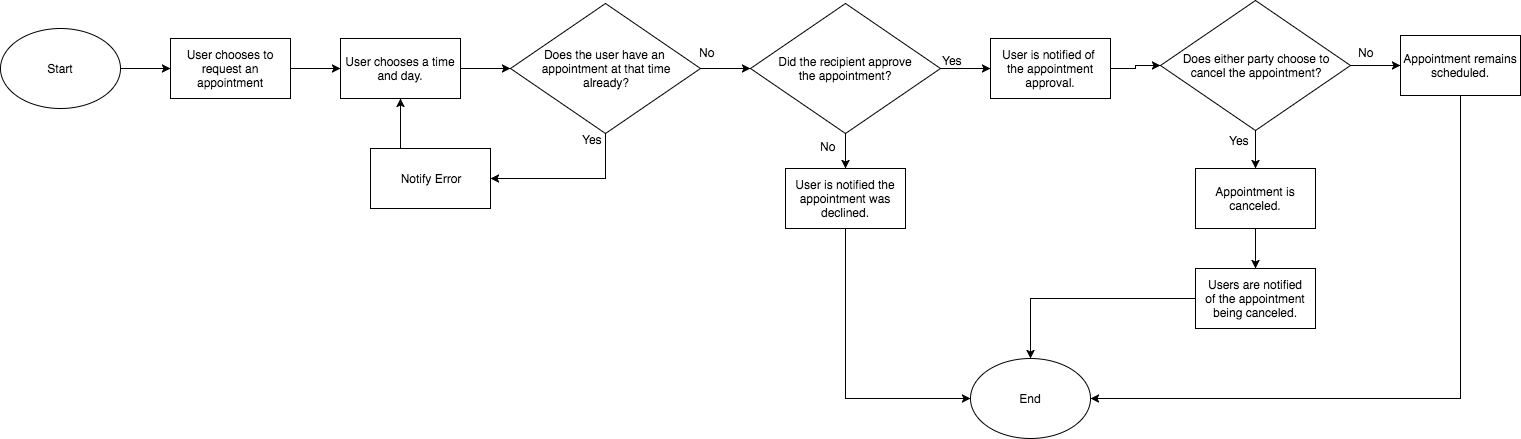
Medical professional and patient can cancel scheduled appointments.

* Appointments must be canceled at least 24 hours in advance to the date and time they were scheduled.

Postcondition (Success): Both the patient and medical professional are able to send, approve, and deny appointment requests. Once the accepting party reaches a decision about the status of the appointment, it should reflect on their calendar, such that if they approve the appointment it will show the scheduled appointment at the scheduled time, otherwise it will not show up. If the appointment was canceled, it should no longer show up on both the patient and the medical professional’s calendar.

Failure: If the appointment is not made when the user has specified, an error message is displayed.

If the appointment is neither approved or denied 24 hours after its request, the appointment will not show up on either party’s treatment plan.



### 

### 

### **Data Analysis Report**

**Business Requirement**: A medical professional needs a graphical way to see the aggregation of their patient(s) data.

Actors: Medical Professional

Precondition:The medical professional is active on the system and has at least one patient assigned to them.

User Story:As a medical professional, I would like a graphical way to see my patient’s participation in the treatments I assign to them and to see the status of their medical condition over time.

Functional Requirement(s) and Criteria:

Medical professional can see data for each individual patient.

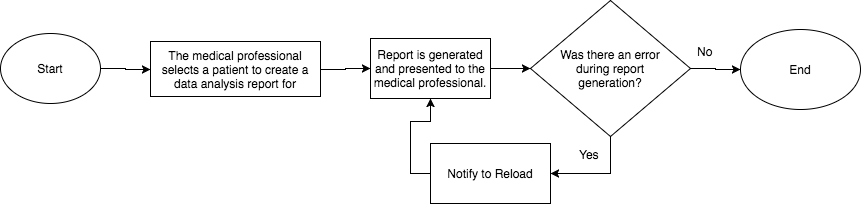
* Medical professional can see graphical representations of the patient’s various stats over a period of time.
* Medical professional can see auto-calculated key quality metrics for a patient.

Medical professional can see aggregated data from multiple patients.

* Medical professional can see graphical representations of patients with a common diagnosis over time on the same data analysis report.

Postcondition (Success): The medical professional can view all aggregated data of his/her patient(s) with common disorders.

Failure: If the medical professional cannot view the graphical representations of a patient, then they will be prompted to refresh the page.



# **Glossary**

**Alpha Characters** - ISO basic Latin alphabet consisting of 26 letters [A-Z a-z] that each have an uppercase and lowercase form.

**Covered Entity** - individuals or organizations that transmit, store, and access a patient’s protected health information.

**Domain** - a distinct subset of the Internet with addresses sharing a common suffix or under the control of a particular organization or individual. In this document, the word *domain* is used to describe the entity or organization that provides an email service. Examples include, but are not limited to Gmail, Yahoo Mail, and Outlook.

**Medical Professional** - an individual who provides medical care and advice to a patient

**Numeric Characters** - a digit or set of digits from the Hindu-Arabic numeral system ranging from 0-9

**Protected Health Information (PHI)** - any information that refers to an individual's demographic data, medical history, laboratory results, insurance information, and any other data that a covered entity holds which can be used to identify the individual

**Session Inactivity** - a state of being idle while using the system. Examples include, but are not limited to periods with no mouse movement on the page or keyboard input on the page

**Treatment Plan** - a systematic schedule of procedures and activities designed for a patient to restore and improve their overall health