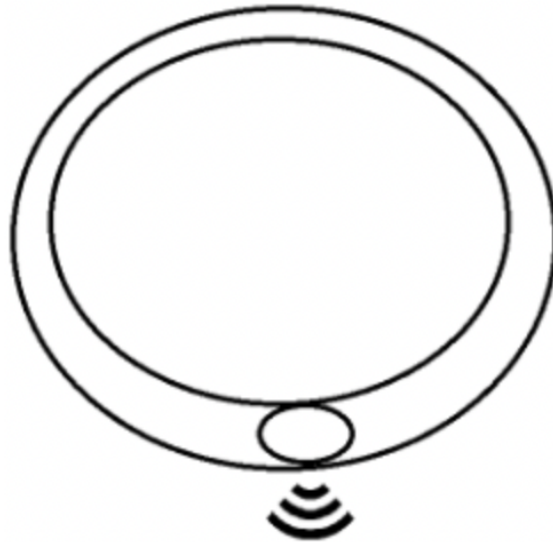


**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
THE UNIVERSITY OF TEXAS AT ARLINGTON**

**SYSTEM REQUIREMENTS SPECIFICATION
CSE 4316: SENIOR DESIGN I
FALL 2022**



**MEDI ID
MEDICAL ID BRACELET**

**AHAMAD NATSHEH
MAHMOUD NATSHEH
ALEX STRINGER
IVAN CHU
CHRISTIAN BLUNDELL**

REVISION HISTORY

Revision	Date	Author(s)	Description
0.1	10.03.2022	AN	document creation
0.2	10.15.2022	AN, MN, AS, IC, CB	complete draft
0.3	10.17.2022	AN	release candidate 1
1.0	12.04.2022	MN	Finalize
2.0	4.05.2023	IC	Updated Version

CONTENTS

1	Product Concept	8
1.1	Purpose and Use	8
1.2	Intended Audience	8
2	Product Description	9
2.1	Features & Functions	9
2.2	External Inputs & Outputs	9
2.3	Product Interfaces	10
3	Customer Requirements	11
3.1	Scan Feature	11
3.1.1	Description	11
3.1.2	Source	11
3.1.3	Constraints	11
3.1.4	Standards	11
3.1.5	Priority	11
3.2	Admin Email Requirement for New Registration Process	11
3.2.1	Description	11
3.2.2	Source	11
3.2.3	Constraints	12
3.2.4	Standards	12
3.2.5	Priority	12
3.3	User Login	12
3.3.1	Description	12
3.3.2	Source	12
3.3.3	Constraints	12
3.3.4	Standards	12
3.3.5	Priority	12
3.4	Update Medical and Patient Records	12
3.4.1	Description	12
3.4.2	Source	12
3.4.3	Constraints	12
3.4.4	Standards	12
3.4.5	Priority	13
3.5	Image Uploading	13
3.5.1	Description	13
3.5.2	Source	13
3.5.3	Constraints	13
3.5.4	Standards	13
3.5.5	Priority	13
3.6	Splash-Proof Requirement for Bracelet	13
3.6.1	Description	13
3.6.2	Source	13
3.6.3	Constraints	13
3.6.4	Standards	13
3.6.5	Priority	13

4	Packaging Requirements	14
4.1	Packaging	14
4.1.1	Description	14
4.1.2	Source	14
4.1.3	Constraints	14
4.1.4	Standards	14
4.1.5	Priority	14
5	Performance Requirements	15
5.1	Website	15
5.1.1	Description	15
5.1.2	Source	15
5.1.3	Constraints	15
5.1.4	Standards	15
5.1.5	Priority	15
5.2	Durable Bracelet	15
5.2.1	Description	15
5.2.2	Source	15
5.2.3	Constraints	15
5.2.4	Standards	15
5.2.5	Priority	15
5.3	Database	15
5.3.1	Description	15
5.3.2	Source	15
5.3.3	Constraints	15
5.3.4	Standards	16
5.3.5	Priority	16
6	Safety Requirements	17
6.1	Usage	17
6.1.1	Description	17
6.1.2	Source	17
6.1.3	Constraints	17
6.1.4	Standards	17
6.1.5	Priority	17
6.2	NFC chip stored securely in the bracelet	17
6.2.1	Description	17
6.2.2	Source	17
6.2.3	Constraints	17
6.2.4	Standards	17
6.2.5	Priority	17
6.3	Material of the Bracelet	17
6.3.1	Description	17
6.3.2	Source	17
6.3.3	Constraints	17
6.3.4	Standards	17
6.3.5	Priority	18

7	Security Requirements	19
7.1	Account creation	19
7.1.1	Description	19
7.1.2	Source	19
7.1.3	Constraints	19
7.1.4	Standards	19
7.1.5	Priority	19
7.2	Password encryption	19
7.2.1	Description	19
7.2.2	Source	19
7.2.3	Constraints	19
7.2.4	Standards	19
7.2.5	Priority	19
8	Maintenance & Support Requirements	20
8.1	User's manual	20
8.1.1	Description	20
8.1.2	Source	20
8.1.3	Constraints	20
8.1.4	Standards	20
8.1.5	Priority	20
8.2	Account setup Video	20
8.2.1	Description	20
8.2.2	Source	20
8.2.3	Constraints	20
8.2.4	Standards	20
8.2.5	Priority	20
9	Other Requirements	21
9.1	Available Network Connectivity Requirement	21
9.1.1	Description	21
9.1.2	Source	21
9.1.3	Constraints	21
9.1.4	Standards	21
9.1.5	Priority	21
9.2	Key Assignment to individual NFC Bracelet User	21
9.2.1	Description	21
9.2.2	Source	21
9.2.3	Constraints	21
9.2.4	Standards	21
9.2.5	Priority	21
10	Future Items	22
10.1	Medical Representative ID Verification for Account Initialization	22
10.1.1	Description	22
10.1.2	Source	22
10.1.3	Constraints	22
10.1.4	Standards	22

10.1.5 Priority	22
10.2 Optical Character Recognition	22
10.2.1 Description	22
10.2.2 Source	22
10.2.3 Constraints	22
10.2.4 Standards	22
10.2.5 Priority	22
10.3 Saved Credentials for Faster Login	23
10.3.1 Description	23
10.3.2 Source	23
10.3.3 Constraints	23
10.3.4 Standards	23
10.3.5 Priority	23

LIST OF FIGURES

1	Medical ID bracelet conceptual drawing	8
2	login screen of the application	10
3	register screen of the application	10
4	Medical information screen of the application	10

1 PRODUCT CONCEPT

This section describes the purpose, use, and intended user audience for the medical ID bracelet product. The Medical ID bracelet is a system that performs easy and secure access to medical information storage. Users of the Medical ID bracelet will be able to wear a bracelet device that contains their medical ID information at all times, which will aid in providing important information needed by medical professionals.

1.1 PURPOSE AND USE

The product Medical ID bracelet should store important medical information about a user that is helpful to medical professionals. The bracelet will be used in the manner of taping the bracelet where the user or medical professional is redirected to a page to log in or register, from there once verified, the user or medical professional will have access to the medical information on the bracelet, the user or medical professional can upload information on the bracelet as they see fits. The bracelet's intended purpose is to help medical professionals understand a user's medical history when assisting the patient and to help EMT workers understand a patient's medical history in the case of the user being passed out and can't communicate to the EMT of previous medical history.

1.2 INTENDED AUDIENCE

The intended audience is both medical facilities and their patients. If the product were to be made available publicly or commercially, the bracelet would be available for purchase by the patients of medical facilities. The bracelet is designed for an overall class of customers since everyone has medical history important for a medical professional to know about before they can help a patient (for example, X-Rays or previous blood work).

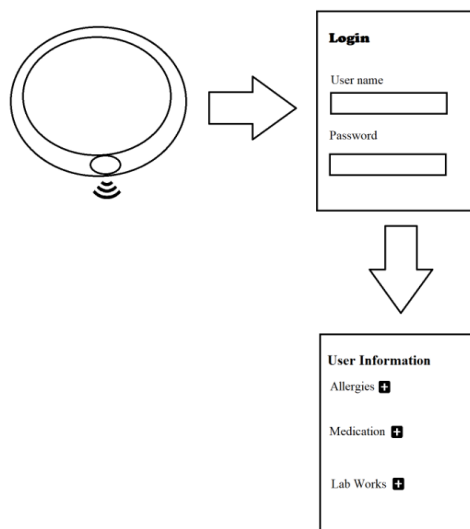


Figure 1: Medical ID bracelet conceptual drawing

2 PRODUCT DESCRIPTION

This section provides the reader with an overview of the medical ID bracelet. The primary operational aspects of the product, from the perspective of end users, maintainers, and administrators, are defined here. The key features and functions found in the product, as well as critical user interactions and user interfaces, are described in detail.

2.1 FEATURES & FUNCTIONS

The medical ID bracelet stores medical information about users and provides security for the data stored on the bracelet. The medical ID bracelet does not act as a medical assistant, nor does it call medical assistance. As seen in Figure 1, the product will be a bracelet for the user to wear on their wrist. The bracelet will have an NFC inserted into the front of it where it is most visible. The bracelet will be tapped by a phone and redirect the phone to a login screen; this will be made possible by the NFC inside the bracelet transmitting to the tapped phone a redirect link. Once the login screen verifies the user or medical professional, it will redirect them to another webpage where they will see the user's medical history/information, as seen in figure 1. Once on the user information page, there will be a plus button beside each section for the user or medical professional to add information. As seen in figure 1, the external elements include the internet and redirect website links as the login screen and medical information data will be on website pages.

2.2 EXTERNAL INPUTS & OUTPUTS

1) Name: Username. Description: The user will log in or register by inputting their username in the username tab on the login or registration page. This will help validate whether the user trying to log in to the app is a user or a medical professional. Use: This will help keep the user's medical information safe and not allow unauthorized users to see the medical information of others.

2) Name: Password. Description: The user will log in or register by inputting their password to their account in the password tab on the login page or registration page. This will help verify that the person claiming to be a specific user is who they claim to be. Use: This will help keep the user's medical information safe and not allow unauthorized users to see the medical information of others.

3) Name: Full Name. Description: The user will create a new account by inputting their name into the name tab on the registration page. Use: This will allow the medical workers to know who the patient is.

4) Name: Date of birth. Description: The user will create a new account by inputting their date of birth into the date of birth tab on the registration page. Use: This will allow the medical workers to know how old the patient is.

5) Name: Email. Description: The user will create a new account by inputting their email into the email tab on the registration page. Use: This will allow the system to send the user updates and the medical facilities to have the patient's email for updates.

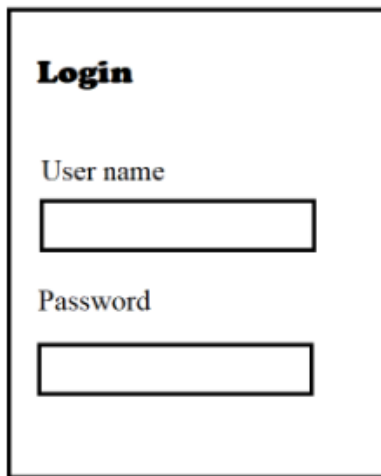
6) Name: Phone Number. Description: The user will create a new account by inputting their phone number into the phone number tab on the registration page. Use: This will allow the system to send the user updates and the medical facilities to have the patient's phone number for updates.

7) Name: Medical information. Description: The user will input important medical information for the medical professionals. Use: This will help the medical professionals understand a patient's medical

history before helping a patient.

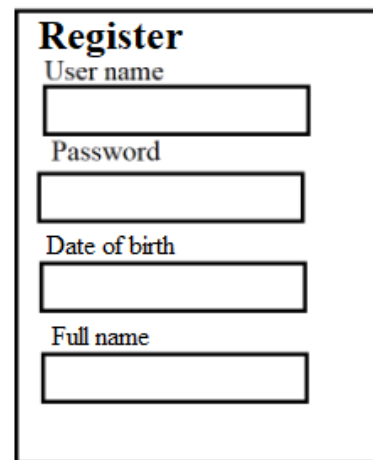
2.3 PRODUCT INTERFACES

There are three main operational (visible) interfaces to the end-user, administrators, maintainers, etc. The first interface is the login screen, as seen in figure 2 below; the login screen will prompt the user to input their username and password, where the user can click the login button at the bottom of the screen and login. The second interface is the registration screen, as seen in figure 3 below; it will prompt the user to input a username, password, full name, date of birth, phone number, and email. At the bottom of the registration screen, there will be a register button where the user can click register, and a new account will be created. The last interface is the medical information screen, as seen in figure 4 below; this screen will show all the medical information related to the user and sort the information by sections (for example, X-Rays and allergies will be two different sections). They will also see a plus button beside each section where they can add more information to the specific section.



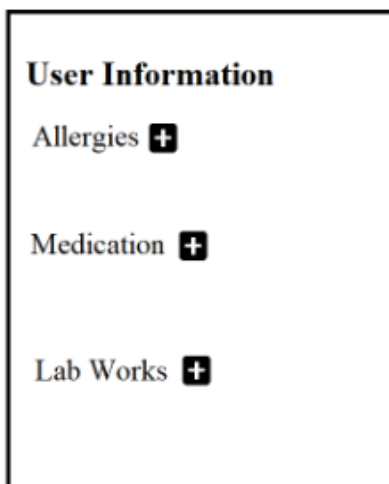
The login screen is a rectangular box with a black border. At the top left, the word "Login" is written in bold black font. Below it, the text "User name" is followed by a horizontal input field. Further down, the text "Password" is followed by another horizontal input field.

Figure 2: login screen of the application



The register screen is a rectangular box with a black border. At the top left, the word "Register" is written in bold black font. Below it, the text "User name" is followed by a horizontal input field. Then, the text "Password" is followed by a horizontal input field. Below that, the text "Date of birth" is followed by a horizontal input field. Finally, the text "Full name" is followed by a horizontal input field.

Figure 3: register screen of the application



The medical information screen is a rectangular box with a black border. At the top left, the text "User Information" is written in bold black font. Below it, the text "Allergies" is followed by a small black square containing a white plus sign. Further down, the text "Medication" is followed by a similar black square with a white plus sign. At the bottom, the text "Lab Works" is followed by another black square with a white plus sign.

Figure 4: Medical information screen of the application

3 CUSTOMER REQUIREMENTS

Team Medi ID will implement four customer requirements for our sponsor. The first customer requirement will be a tap feature. This feature will allow a user to take their phone and tap one of our medical identification bracelets, once the NFC in the medical identification bracelet detects the phone it will redirect the user to our website that will require the user to login and verify their credentials in order to gain access to the user's medical records. The NFC will carry two key pieces of information the first being the link to our website, and the second being a key to the owner of the bracelets account. The second user requirement is to have users create accounts. This will be a two-system setup where either user can sign up to be medical physicist /EMT or a patient. The third user requirement will be a login, this is in order to have some security and not just allow anyone who taps a medical bracelet to gain access to medical information. The last customer requirement is to have users be able to add and update medical information on our online website.

3.1 SCAN FEATURE

3.1.1 DESCRIPTION

The scan feature will allow a user to take their phone and tap one of our medical identification bracelets, once the NFC in the medical identification bracelet detects the phone it will redirect the user to our website that will require the user to login and verify their credentials in order to gain access to the users medical records. The NFC will carry two key pieces of information the first being the link to our website, and the second being a key to the owner of the bracelets account.

3.1.2 SOURCE

The source of this requirement comes from our sponsor which is our senior design professor Shawn Gieser.

3.1.3 CONSTRAINTS

The only constraint with this tap feature is security. In order to combat any security risk of having anyone tap a medical identification bracelet and having access to private medical information we are adding a login for each account which prevents people from getting access without being the right user to use it.

3.1.4 STANDARDS

Not applicable.

3.1.5 PRIORITY

The priority of this requirement is critical as the tap feature is the whole project. If a user cannot tap a medical identification bracelet and be redirected to their medical information this product will be a failure.

3.2 ADMIN EMAIL REQUIREMENT FOR NEW REGISTRATION PROCESS

3.2.1 DESCRIPTION

The second requirement is to implement an admin email requirement for the new registration process. When a user creates a new account, an email notification will be sent to the admin email address. The admin will then verify the user's account before granting access to the system. This will help to ensure the security and privacy of users' medical information.

3.2.2 SOURCE

Professor Shawn Gieser

3.2.3 CONSTRAINTS

Not applicable.

3.2.4 STANDARDS

Not applicable.

3.2.5 PRIORITY

The priority of this requirement is critical. Without an admin email requirement, there is a risk that unauthorized users could gain access to sensitive medical information. By implementing an admin email requirement, we can ensure that all user accounts are verified and approved before granting access to the system. This will help to prevent security breaches and protect the privacy of our users.

3.3 USER LOGIN

3.3.1 DESCRIPTION

The next user requirement will be a login, this is in order to have some security and not just allow anyone who taps a medical bracelet to gain access to medical information.

3.3.2 SOURCE

The source of this requirement comes from our sponsor which is our senior design professor Shawn Gieser.

3.3.3 CONSTRAINTS

Not applicable.

3.3.4 STANDARDS

Not applicable.

3.3.5 PRIORITY

The priority of this requirement is high. The reason for this is because if there is no login then no one will be able to gain access to the patient's medical record and the product will be worthless. Also, if there is no login then there will be no security implemented in the product and no one will use the product since their medical information will not be secure.

3.4 UPDATE MEDICAL AND PATIENT RECORDS

3.4.1 DESCRIPTION

The last customer requirement is to have users be able to add and update medical information on our online website. This will allow users to add a variety of information for example, Name, date of birth, patient information, primary care physician, medical records, medical conditions, and other medical related documents.

3.4.2 SOURCE

The source of this requirement comes from our sponsor which is our senior design professor Shawn Gieser.

3.4.3 CONSTRAINTS

Not applicable.

3.4.4 STANDARDS

Not applicable.

3.4.5 PRIORITY

The priority of this requirement is critical. The reason for this is if we cannot store medical information then there is no use for the product, and no one will use it as its main feature which is storing medical records will not be available.

3.5 IMAGE UPLOADING

3.5.1 DESCRIPTION

Image uploading is a feature that allows users to upload images or photos to a software system.

3.5.2 SOURCE

Shawn Gieser

3.5.3 CONSTRAINTS

Not applicable.

3.5.4 STANDARDS

Not applicable.

3.5.5 PRIORITY

Low

3.6 SPLASH-PROOF REQUIREMENT FOR BRACELET

3.6.1 DESCRIPTION

The bracelet must be designed and manufactured to be splash-proof. This means that it must be able to withstand exposure to water and other liquids without suffering damage or malfunctioning.

3.6.2 SOURCE

Shawn Gieser

3.6.3 CONSTRAINTS

The device must remain functional and accurate despite exposure to water or other liquids

3.6.4 STANDARDS

The device must meet the International Electrotechnical Commission (IEC) standard 60529 for ingress protection, specifically IP67 or higher.

3.6.5 PRIORITY

The priority of this requirement is high. The bracelet will be used in a variety of settings and environments, and it is important that it can withstand exposure to water or other liquids without becoming damaged or malfunctioning. Failure to meet this requirement could result in significant damage to the device and compromise its effectiveness in gathering and transmitting medical data.

4 PACKAGING REQUIREMENTS

The medical identification bracelet will be packaged in a rectangular white box that reads Medi ID on it. The box will be two pieces a bottom half where the medical identification bracelet will be placed and a top half where you can slide it off. Once the user opens the box inside will be the medical identification bracelet and a small user manual on how to set up their new bracelet and how it works.

4.1 PACKAGING

4.1.1 DESCRIPTION

The medical identification bracelet will be packaged in a white rectangular box. On the top of the box, it will say Medi ID on it. Inside the packaging will be the medical identification bracelet and a user guide on how to set it up.

4.1.2 SOURCE

The source of this requirement comes from our whole team Medi ID.

4.1.3 CONSTRAINTS

Not applicable.

4.1.4 STANDARDS

Not applicable.

4.1.5 PRIORITY

The priority of this requirement is low. The reason for this is because if we do not package it in this packaging it will not affect the usability of the product.

5 PERFORMANCE REQUIREMENTS

Clients should be able to access the website once the bracelet is scanned. The bracelet should also be durable for the users to wear it for a long time. The website that opens after the bracelet is scanned should contain the wearer's information. The client should also be able to edit their information with the confirmation of a doctor. Time to set up and battery are not required.

5.1 WEBSITE

5.1.1 DESCRIPTION

A website that shows the client's information should be open once the clients scanned their bracelets.

5.1.2 SOURCE

Sponsor

5.1.3 CONSTRAINTS

N/A

5.1.4 STANDARDS

N/A

5.1.5 PRIORITY

Moderate

5.2 DURABLE BRACELET

5.2.1 DESCRIPTION

A durable bracelet that can be worn for a long period of time.

5.2.2 SOURCE

Sponsor

5.2.3 CONSTRAINTS

N/A

5.2.4 STANDARDS

N/A

5.2.5 PRIORITY

Moderate

5.3 DATABASE

5.3.1 DESCRIPTION

A database to store the client's information.

5.3.2 SOURCE

Sponsor

5.3.3 CONSTRAINTS

N/A

5.3.4 STANDARDS

N/A

5.3.5 PRIORITY

Moderate

6 SAFETY REQUIREMENTS

To make sure the bracelet is safe enough for public use, the NFC chip will be stored securely in the bracelet to prevent the users consume it by accident.

6.1 USAGE

6.1.1 DESCRIPTION

A manual will be provided to display the way of using the bracelet

6.1.2 SOURCE

Sponsor

6.1.3 CONSTRAINTS

N/A

6.1.4 STANDARDS

N/A

6.1.5 PRIORITY

Critical

6.2 NFC CHIP STORED SECURELY IN THE BRACELET

6.2.1 DESCRIPTION

The NFC chip should be stored securely in the bracelet to prevent the users consume it by accident.

6.2.2 SOURCE

Sponsor

6.2.3 CONSTRAINTS

N/A

6.2.4 STANDARDS

N/A

6.2.5 PRIORITY

Critical

6.3 MATERIAL OF THE BRACELET

6.3.1 DESCRIPTION

Non-toxic silicone environmental protection material will be used to protect the users.

6.3.2 SOURCE

Sponsor

6.3.3 CONSTRAINTS

N/A

6.3.4 STANDARDS

N/A

6.3.5 PRIORITY

Critical

7 SECURITY REQUIREMENTS

For security, each user will have their own account to add their personal information. Each user will need to create a username and a password to sign into their account. Each time medical personnel use their phone to tap the NFC chip they will be led to a login page; they then must sign in with their own credentials. All hospitals and medical personnel must be verified after registration.

7.1 ACCOUNT CREATION

7.1.1 DESCRIPTION

Each user must create an account. To login to their account the user must create a username and password. This allows the users account information to be protected from unauthorized users. Hospitals and medical personnel must undergo a verification process, in order to see patients information.

7.1.2 SOURCE

Source

7.1.3 CONSTRAINTS

Password must follow password requirements: Must have one uppercase and lowercase, one special character, and at least 10 characters long. Must manually verify hospitals and medical personnel.

7.1.4 STANDARDS

Must follow safe password requirements

7.1.5 PRIORITY

High

7.2 PASSWORD ENCRYPTION

7.2.1 DESCRIPTION

All data including passwords, login information, and user data will be stored in a database. Each password will be salted hashed, and encrypted to prevent credentials from being used. User personal information will be encrypted. This is keeping the users information safe in the case of a data breach

7.2.2 SOURCE

Source

7.2.3 CONSTRAINTS

Must follow NIST Special Publication 800-63B guidelines to prevent possible data breaches.

7.2.4 STANDARDS

NIST Special Publication 800-63B

7.2.5 PRIORITY

High

8 MAINTENANCE & SUPPORT REQUIREMENTS

To support users in their account creation process, we will supply a user's manual with the bracelet. This manual will guide the user step-by-step in creating an account with basic information. After, they then can add any additional information that they would want to share to their account. If the NFC chips is defective, another bracelet will be sent to the user after they contact support. All documentation of source code and NFC writing tool will be available to the software development team.

8.1 USER'S MANUAL

8.1.1 DESCRIPTION

The user's manual contains instructions on how to set up the medical bracelet. The manual will guide the user step-by-step through account creation and linking the account to the bracelet. The steps will be accompanied by small diagrams to help guide the user. The user manual will also have a few other translations for users who do not speak English.

8.1.2 SOURCE

Source

8.1.3 CONSTRAINTS

Only a limited number of translations will be printed onto the manual.

8.1.4 STANDARDS

IEC/IEEE 82079

8.1.5 PRIORITY

Low

8.2 ACCOUNT SETUP VIDEO

8.2.1 DESCRIPTION

This video follows the step-by-step guide of the user's manual. The video provides a visual representation on how to set up and link one's account. The video will show the bracelet and web page, while on the web page the video guides the new user to the account creation page. After the user has registered and logged in the video gives a brief explanation on what information can be added to the user's account.

8.2.2 SOURCE

source

8.2.3 CONSTRAINTS

Video will only be available in English and no other language. Audio and video quality must be good enough to understand what is said and clear enough to see what is happening.

8.2.4 STANDARDS

8.2.5 PRIORITY

Low

9 OTHER REQUIREMENTS

Connection to a network is required in order to set up a patient account as well as to verify EMT/hospital accounts. A key is required for each NFC bracelet in order to complete the verification of the targeted access user, which is randomly generated after the user initializes an account.

9.1 AVAILABLE NETWORK CONNECTIVITY REQUIREMENT

9.1.1 DESCRIPTION

A network is required to successfully submit patient information or retrieve that information. The network is used to register accounts, verify accounts, log into accounts, or access the database. Without access to a network, the database nor the account can be retrieved or updated on either end (patient or EMT).

9.1.2 SOURCE

Sponsor (S. Gieser) and all team members

9.1.3 CONSTRAINTS

Financial constraints of either user end: user or medical representative may not have immediate network access at all times.

9.1.4 STANDARDS

RFC 9314 and previous [w], including initial internet standards (TCP, HTTP, TLS, OSI, UDP)

9.1.5 PRIORITY

Crucial

9.2 KEY ASSIGNMENT TO INDIVIDUAL NFC BRACELET USER

9.2.1 DESCRIPTION

A key must be assigned to each NFC bracelet to personalize the hardware and configure an assignment of sensitive user information to the correct user. The medical representative uses this key to verify the correct patient information is retrieved, in order to prevent misunderstanding of individual medical cases. Without the assignment of a key, the user data will be at risk of unsolicited retrieval from third parties, misuse of patient information by unverified medical representatives, and access to other information on the user's NFC bracelet.

9.2.2 SOURCE

Sponsor (S. Gieser)

9.2.3 CONSTRAINTS

Technological Constraints such as large-scale testing of key security in NFC bracelets are present since the team cannot get access to several user accounts and individual NFC bracelets with individually assigned keys. Legal Constraints may also arise when testing key security with medical facility verification since medical facilities have strict privacy protection policies that they must follow before releasing information needed to verify patient data.

9.2.4 STANDARDS

CNSSI 4009 [x]

9.2.5 PRIORITY

High

10 FUTURE ITEMS

Future requirements include verification for medical representatives and interactive sharing of additional optional patient information. Due to various constraints that require extensive time, cost, and technological implementation, these requirements are considered to not be in scope of the project based on the defined time frame.

10.1 MEDICAL REPRESENTATIVE ID VERIFICATION FOR ACCOUNT INITIALIZATION

10.1.1 DESCRIPTION

Just like the user, a medical representative must include codes similar to an ID that determines the unique user initialization. Medical facilities or representatives when initializing their account to access user information must enter a unique ID to ensure that they are qualified medical professionals that are legally allowed to view medical information about specific users. Without this method of verification, it may be unsure if the right representatives are accessing sensitive medical information of others.

10.1.2 SOURCE

Sponsor (S. Gieser)

10.1.3 CONSTRAINTS

Since each medical facility/representative operates in a unique environment based on the health service they work for in the United States, it is difficult to identify a common "ID" code that can be immediately verified during account initialization. Each health care service has different account number types for representatives, and some medical facilities may not even have an identifying code that they can provide to verify accounts for those that work at that facility.

10.1.4 STANDARDS

Standards: ISO/IS 20302, ISO/TS 18530 [y]

10.1.5 PRIORITY

Future

10.2 OPTICAL CHARACTER RECOGNITION

10.2.1 DESCRIPTION

It is a technology that enables the recognition and translation of printed or handwritten text characters into machine-readable text. OCR is often used to convert scanned documents, PDFs, images, or other forms of text into digital format that can be edited, searched, and analyzed by computers.

10.2.2 SOURCE

Sponsor (S. Gieser)

10.2.3 CONSTRAINTS

N/A

10.2.4 STANDARDS

High level of Accuracy, Language Support, Font Recognition, and Compatibility

10.2.5 PRIORITY

Future

10.3 SAVED CREDENTIALS FOR FASTER LOGIN

10.3.1 DESCRIPTION

This feature allows users to save their login credentials (such as username and password) or use biometric authentication methods (such as Touch ID or Face ID) to quickly and easily access their accounts without having to enter their login information every time they use the app.

10.3.2 SOURCE

Christian

10.3.3 CONSTRAINTS

The security of saved credentials must be ensured, with appropriate measures in place to protect against unauthorized access or theft of user data.

10.3.4 STANDARDS

Compliance with industry standards for password and biometric authentication security, such as those outlined by the National Institute of Standards and Technology (NIST).

10.3.5 PRIORITY

High, as this feature can greatly enhance user experience and convenience. However, security concerns must be thoroughly addressed before implementation.

REFERENCES