CSE 345/545 Foundations of Computer Security

Course Project

Patient Data Management System

1. Introduction

A patient data management system is a software system developed primarily to facilitate the verification of the patients' documents while buying medicines or making medical claims.

The focus of this project is to develop a portal that facilitates the secure exchange and verification of electronic health records. This document shall be used as a set of guidelines. You can make necessary additions and changes to the requirements with prior written approval from the Professor.

2. Requirements

A user should be able to use this system at any place and any time with the availability of the internet and web browsers. In addition to the requirements mentioned below, all the global standards/laws concerning healthcare websites should be strictly followed.

2.1. Users

Each user (except the admin) will upload documents (proof of identity/address/health licenses) and request the admin's approval to use the system. Once the admin approves the users, they can use the platform.

2.1.1. Patients

A patient can access a catalog of healthcare professionals and organizations. The user can search for a specific healthcare professional or organization on the website. The user can also apply location filters.

A patient can request health records from any healthcare professional or hospital, buy medicines/drugs from any pharmacy, and claim medical reimbursement from any insurance firm. To purchase medicines/drugs and claim medical refunds, the user will first provide the appropriate documents to the respective organizations. The documents can involve doctors' prescriptions, discharge summaries, test results, hospital bills, medical bills, etc. Only after verification of those documents can they proceed further.

You must mimic a payment gateway for all the transactions; both CRUD-based and third-party providers (e.g., stripe, Razorpay, etc.) are acceptable.

2.1.2. Healthcare professionals

A healthcare professional can provide the appropriate patient with prescriptions, clinical findings, test results, bills, etc.

2.1.3. Admin

An admin can remove any suspicious user or organization from the platform. The admin can also approve their applications after reviewing the uploaded documents.

2.2. Organizations

Each organization will upload documents (licenses and permits) and request the admin for approval to use the system. Once the admin approves the organization, they will be allowed to use the platform.

Each organization must have the following information:

- Name
- Description
- At least two images
- Location
- Contact details

You can add additional information if required.

2.2.1. Hospitals

A hospital can provide the appropriate patient with prescriptions, discharge summaries, scans, test results, bills, etc.

2.2.2. Pharmacy

A pharmacy can sell any medicines/drugs to patients with verified prescriptions. Only after verification can they sell the medicines and provide the medical bills to the patients.

2.2.3. Insurance firms

An insurance firm can provide medical claims to patients with verified documents. Only after verification can they proceed with the reimbursement.

2.3. Functionality

Students should decide about suitable access rights/ privileges and other security features. Below are some basic functionality details for this project:

a. Mechanism to search professionals & organizations using type, name, & location.
b. Creation and maintenance of various organizations' lists.
c. Ability to set/edit settings.
d. Ability to delete their own medical records.
e. An e-cash wallet (or a payment gateway) for performing financial transactions.

f. Maintenance of profile information of the user/organization.
g. Ability to buy medicines and get medical claims.
h. Ability to provide documents to other users (patients/organizations).
i. Ability to automatically verify the documents.
j. Admin capabilities as mentioned above or more.
k. User-Admin approval process using a document upload.

2.4. Key requirement

- **Document Verification System:** The patients will provide the documents to the healthcare professionals or organizations, which need to verify automatically.

  You can have the following types of verification in the system.

  a. The patients issue verifiable documents and share them with healthcare professionals and organizations.
  b. The healthcare professionals issue verifiable documents and share them with the patients.
  c. Healthcare organizations issue verifiable documents and share them with the patients.

  You can use digital signatures and/or blockchain to share & verify the documents. If required, you can also use the metadata information instead of the whole document.

2.5. Other Requirements

- **Public Key Certificates:** The secure healthcare website must use public key infrastructure (PKI) and SSL/TLS (HTTPS) to enforce the application's security. You can establish your own certificate issuing authority for this project. A minimum of two functions must employ PKI, and you may decide the extent of the PKI applicability to the functions.
- **OTP:** The secure healthcare website must employ OTP (One Time Password) technique with a virtual keyboard feature to validate highly sensitive transactions for at least two of the functions in requirements. You may decide the extent of the OTP applicability to the functions.
- The secure healthcare website should allow multiple users to use the system simultaneously.
- Secure transaction logging is required to enable external audits.
- Must employ security features to defend against attacks on the secure healthcare website (the TAs and students will test the project).
- Make sure you read about payment gateway compliance and store only the data allowed to be stored. For example, keeping card details and private keys on your local database is not permitted.

3. Programming Languages and Framework

Each group can choose the programming language of their preference through consensus. Each group can use the following: OS: Windows (XP or any newer version) or Linux. DBMS: MySQL, Mongo DB, SQLite, or Postgres. Web server: Nginx, IIS, or Apache. However, if you choose to use other types of OS, database systems, or web servers for the project, you need to discuss it with the TA since the TA may be unable to help you with the project.

4. Milestones

The TAs will continuously evaluate your progress in weekly meetings. Groups will be required to demo their project to their TAs at the end of each month and will be graded according to the following milestones:

- September Milestone [2.5%]
    - Decide the full tech stack, including OS, web server, and database (a rough idea).
    - Install and configure the web server along with SSL/TLS certificates.
    - Host any sample **HTTPS** website on the VM provided.
- October Milestone [2.5%]
    - Host an HTTPS website on the web server that enables the following functionalities
        - Users of all categories can log in/signup on to the website to view and edit their profile information.
        - Patients can view and search through a catalog of healthcare professionals and organizations.
        - Users can upload and share documents with other users.
        - Users can delete their own documents.
        - A payment gateway system for buying medicines and claiming medical refunds
        - Patients can issue and share verifiable documents with healthcare professionals & organizations. (**Part a.** of the Document Verification System mentioned above)
        - Admin approval system as mentioned above.
        - Admin can remove any suspicious patient or organization from the platform.

      In addition, the website must also use OTP for at least two of the functions in the requirements.
    - Finalize your tech stack and VM requirements. *No changes to these will be accepted after October.*

IMPORTANT: **7.5% BONUS marks** will be awarded to the groups who have used blockchain for the automatic verification system in the final submission.