ITMB
COC252
F011321

EHR System Modernization in the Republic of Moldova

by

Calin Corcimaru

Supervisor: Dr. Georgina Cosma

Department of Computer Science
Loughborough University

May 2025

Abstract

Abstract to be added

Acknowledgements

Acknowledgements to be added

List of Figures

Contents

Chapter 1

Introduction

1.1 Background

The Republic of Moldova is a small country in Eastern Europe that borders Romania and Ukraine, with a current population of 2.4 million people (**mdpop**). Since its independence in 1991, Moldova has faced a number of challenges, including political instability, corruption, and economic difficulties which have left Moldova as one of the poorest countries in Europe (**mdpoverty**).

Despite these challenges, Moldova has made significant progress in its digital transformation efforts, with the government launching a number of initiatives to modernize its public services and improve the quality of life for its citizens (**mdega**). An example is the Citizen's Government Portal (MCabinet), which allows citizens to access personal information such as 'valid identity documents, social contributions and benefits, own properties, information about the family doctor and the health institution where the person is registered, tax payments and other information about the citizen-government relationship' (**mdcabinet**).

To continue supporting the existing transformation initiatives, Moldova's Cabinet of Ministers has recently approved the 'Digital Transformation Strategy of the Republic of Moldova for 2023-2030', which aims to transform the country into a digital society by 2030, with the ultimate goal of having 'all public services available in a digitalized format' (**mdstrategy**).

1.2 Problem Statement

The healthcare sector in Moldova has also seen some transformations, with the introduction of a new electronic health record system (EHR) in 15 hospitals across the country in 2017, called 'Sistemul informațional automatizat „Asistența Medicală Spitalicească" (SIA AMS)' (**mdehr**). While the system has been successful in helping doctors access patient information more efficiently such as medical history, examinations, test results, and prescriptions, the system hasn't been updated since its inception in 2017 and there are still challenges that need to be addressed in 2024.

The main challenge with the current system lies in the user experience (UX) – SIA AMS feels old and isn't user-friendly, with a clunky interface that is difficult to navigate, not adhering to modern accesibility standards and only accessible via Internet Explorer or legacy version of Microsoft Edge, with no support for other browsers or devices (**mdehr**).

Another big challenge with the system is its lack of interoperability within public and private medical institutions due to a lack of a nationally-wide integrated system – each hospital and clinic have their own, siloed, information system that contains the patient information, with no communication being made between systems in different hospitals (**mdehr**).

Finally, due to the current economic situation in Moldova, the government has not allocated any funds to upgrade the current or develop new systems, and the hospitals and clinics that use the system do not have the resources to update it themselves.

1.3 The Client

The client, "Nicolae Testemiteanu" State University of Medicine and Pharmacy in Moldova (USMF), is a public university in Chisinau, Moldova, that offers a range of medical programs, including medicine, dentistry and pharmacy (**mduni**). Many of the faculty at USMF are also practicing doctors at hospitals and clinics across Moldova, and have first-hand experience with the current IT systems used in both public and private medical institutions. The USMF faculty members that the student will be interacting with during the project are part of an innovation team that researches potential opportunities to improve the healthcare sector in Moldova through the use of technology. As such, the client has expressed a need for a prototype that can act as a proof of concept for a modern system that could either replace or augment the current system in Moldova.

1.4 Project Objectives

This project aims to initially conduct some research on the current situation of the IT systems used in the healthcare sector in Moldova by interviewing several stakeholders from various healthcare-related institutions. Afterwards, the project will conduct a literature review on the most appropriate technologies and methodologies for developing a modernized EHR system, and an analysis of existing EHR systems to identify their existing functionality. Finally, based on the information gathered, the project will focus on designing and developing a working prototype, based on the requirements gathered and the feasibility of the chosen solution for the Moldovan healthcare sector. The student's hope is that the solution can then be used as a proof of concept to secure funding for a full-scale implementation of the new system in Moldova by the relevant authorities, such as the Ministry of Health.

As such, the objectives of the project are as follows:

1. Identify 2 to 4 stakeholders from various perspectives, such as healthcare institutions in Moldova and patients, that can provide insights into the current IT systems used in the healthcare sector in Moldova.
2. Conduct interviews with the identified stakeholders to gather information on the current IT systems used in the healthcare sector in Moldova.
3. Carry out a literature review to research the most appropriate technologies (frontend, backend and database) and project management methodologies for developing a modernized EHR system.
4. Explore at least 2 existing EHR systems and identify their strengths and weaknesses.
5. Design and develop a working web or mobile app for an EHR system based on the requirements gathered and the feasibility of the chosen solution for the Moldovan healthcare sector.
6. Offer the client the prototype to be used as a proof of concept to secure funding for a full-scale implementation of the new system in Moldova.

Chapter 2

Research and Requirements

To gain a more complete understanding of the current situation in Moldova, the existing problems and possible needs of the people involved, it is important to start with an analysis to identify the possible key stakeholders for this project. As previously mentioned in the literature review, a diverse group of stakeholders is essential to ensure that the currrent situation is reviewed from multiple perspectives.

Afterwards, the next step is to utilise the chosen stakeholders to gather as much information as possible from various perspective to ensure that the project is aligned with the needs of both patients and healthcare professionals in Moldova and solves the existing problems.

2.1 Stakeholder Analysis

The student has identified the following possible stakeholders for the project:

- Doctors and other medical staff working in hospitals
- Department head in a hospital
- IT staff members in hospitals
- Staff members at CNAM (National Health Insurance Company)
- Staff members at the Ministry of Health
- Patients

These stakeholders have been identified so that they can provide a wider picture on the needs and requirements of the project, and to ensure that the project is aligned with the

expectations of workers within the healthcare industry in Moldova from multiple perspectives.

The stakeholders have also been placed in the stakeholder influence-interest grid (which will be discussed in section 3.2.2) to help the student understand the level of influence and interest that each stakeholder has in the project:

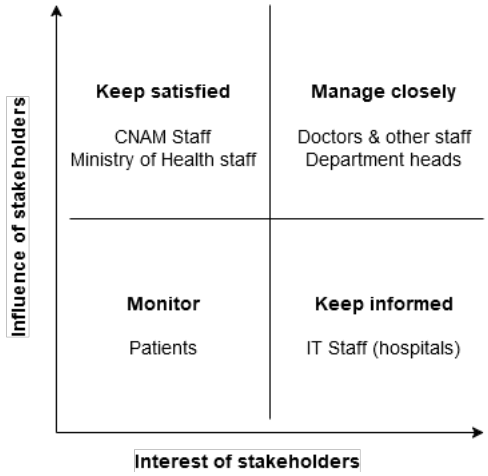


Figure 2.1: Chosen stakeholders in the stakeholder influence-interest grid

2.1.1 Current situation analysis

Following the analysis, the student has conducted several exploratory interviews with the chosen stakeholders to gather insights into current issues with the IT systems used in Moldova's healthcare sector. The student was able to reach out to every stakeholder, except for staff members at CNAM and the Ministry of Health.

After the conclusion of the interviews, three main issues and potential solutions have been identified:

1. Current EHR system is outdated and only accessible via Internet Explorer or legacy version of Microsoft Edge. A potential solution is to develop a new, modernized version of the existing system (retaining the core functionality) that is accessible via modern browsers, is more user friendly and has future upgrade capabilities.

2. Lack of interoperability between medical institutions due to a lack of a nationally-wide integrated system. A potential solution is to create a new system that acts as a patient history archive, where patients can upload their own medical records (such as lab tests, previous medical history, etc) and share them with any medical practitioner,

regardless of the institution they work at.

3. Lack of digitalizion for some systems that still rely on paper-based records or very rudimentary data structures, such as the national transplant registry. A potential solution is digitalized of said system, as is in the case of the transplant registry, that can be accessed by any medical practitioner in Moldova.

Analysing the current issues and potential solutions, the student has determined that the solutions for issues #1 and #3 are too complex, as they require a complete overhaul and integration with existing systems. As such, the student has decided to focus on issue #2, as it is the most feasible and an MVP can be develop within the timeframe of the project.

Consequently, the stakeholder list has been updated to reflect the changed focus of the project:

- Doctors working in hospitals and clinics
- Staff members at the Ministry of Health
- Staff members at CNAM
- Patients that are using both public and private healthcare institutions
- Other medical staff members (nurses, pharmacists, etc)
- Staff members at CNPDCP (National Center for Personal Data Protection)

At the same time, the stakeholder influence-interest grid has been updated to reflect the changes in the project focus:

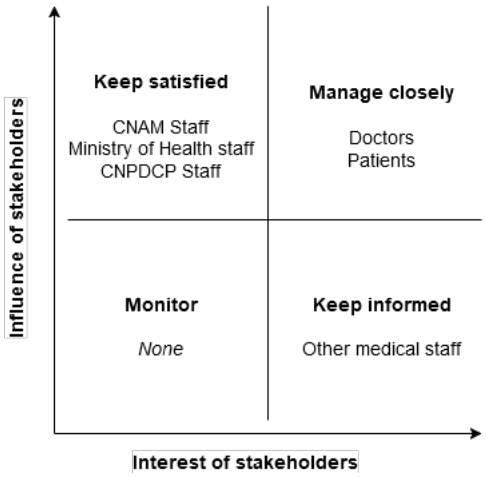


Figure 2.2: Updated stakeholders in the stakeholder influence-interest grid

2.2 Requirements

After the new stakeholders were identified, additional interviews were conducted to focus on the requirements for the chosen solution and enough information was gathered from the other stakeholders to identify the main requirements for the project. The student was unable to reach out to the staff members at CNAM, the Ministry of Health and CNDCP - instead legislation and regulations on their websites were reviewed (**CNAM**; **CNPDCP**; **ministry**).

All of the gathered requirements can be found in the appendix (section A), but the most important requirements have been summarized in the table below:

ID	Category	Requirement
1	Non-functional	The system must be accessible on all modern desktop and mobile-based browsers.
2	Non-functional	The system must store the data in a secure manner, ensuring that only the patient and the doctor can access the data.
3	Document upload	The system must allow patients to upload their own medical records in a variety of formats (PDF, DOC, etc).
4	Personal cabinet	The system must display the patient's history in a chronological order in the form of a timeline.
5	Personal cabinet	The patient personal cabinet must provide an overview of the patient's history through 3 main sections: personal information, lab tests, and doctor consultations.
6	Personal Cabinet	The system must allow patients to add their own personal information, such as name, date of birth, or address.
7	Personal Cabinet	The system must allow patients to add their own allergies and vaccinations.
8	Shareable link	The system must allow the patient to generate a shareable link to provide access to their medical records.
9	Doctor view	When shared with the doctor, the system must allow the doctor to only view the patient's history, not edit it.
10	Patient medication	The system must allow patients to enter their current medication including details such as the name of the drug, dosage, frequency and start/end date.

Table 2.1: Summary of the Most Important Requirements

Chapter 3

Literature Review

This chapter will provide a review of the existing literature, which will be used guide the student in their planning and development efforts of the project.

As such, it will be covering the following areas:

- Software development methodologies
- Requirement and stakeholder management
- Tech stack (backend and frotnend)
- Large Language Models (LLMs)
- PHR Systems

3.1 Software development methodologies

3.1.1 Software Development Life Cycle

The Software Development Life Cycle (SDLC) is a process used to guide the development of software applications or systems (**sdlc1**). The SDLC consists of multiple phases, each with its own set of activities and deliverables. **sdlc2** outline the phases of the SDLC as following:

1. **Requirement gathering and analysis phase** - the requirements are gathered saved in a document. Based on the requirements gathered, a development plan is created.
2. **Design phase** - requirements are written in a more technical manner and system desings are created.

3. **Implementation phase** - Actual development of the software occurs in this phase. Additionally, some smaller unit tests may be done during this phase.
4. **Testing phase** - may involve multiple types of testing, such as unit testing, integration testing, and system testing. **testing** describes the different types of tests:
    - Unit testing - testing individual units or components of the software.
    - Integration testing - performed on two or more units combined together, focusing on the interfaces between these components.
    - System testing - focuses on the 'end-to-end quality of the entire system', testing it as a whole.
5. **Maintenance phase** - involves the deployment and maintenance of the software. Additionally, this phase may include end-user acceptance testing, to ensure that it meets their needs (**testing**).

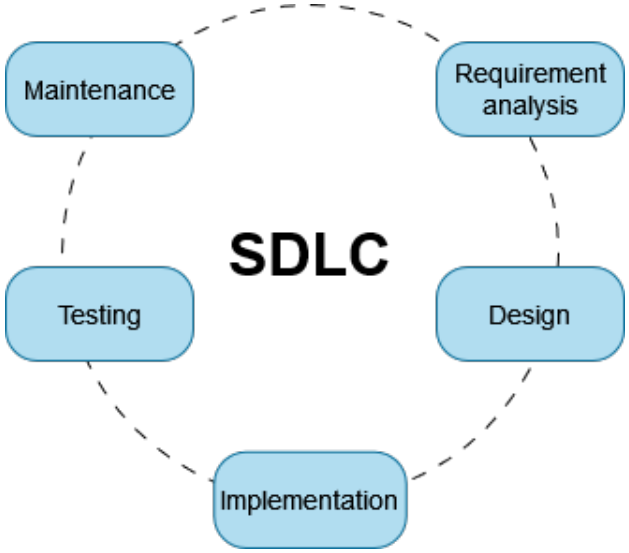


Figure 3.1: Software Development Life Cycle

3.1.2 SDLC Models

The literature describes several SDLC models that have been used in the development of software applications. **sdlc1**; **sdlc2** highlight the most common ones: Waterfall model, V model, Spiral model, Interative model, and Agile model.

Waterfall Model

The Waterfall Model is probably the most well-known SDLC model. It is a linear model, where the development process is divided into distinct, sequential phases (which can be seen in figure 3.2).

The Waterfall Model's strengths lie in its simplicty of use, ease of understanding and a clear, structured approach (**waterfall**). An additional stregth that the authors note is its extensive documentation and planning, emphasizing quality and adherence to regulations.

On the other hand, one of Waterfall's main weaknesses is its lack of flexibility in regards to change (**waterfallno**). Thus, this model is not suitable for projects where the requirements are not well understood or are likely to change. Additionally, the project deliverable is not avaialable until the end of the project, any changed or feedback cannot be done during its development (**waterfallno**).

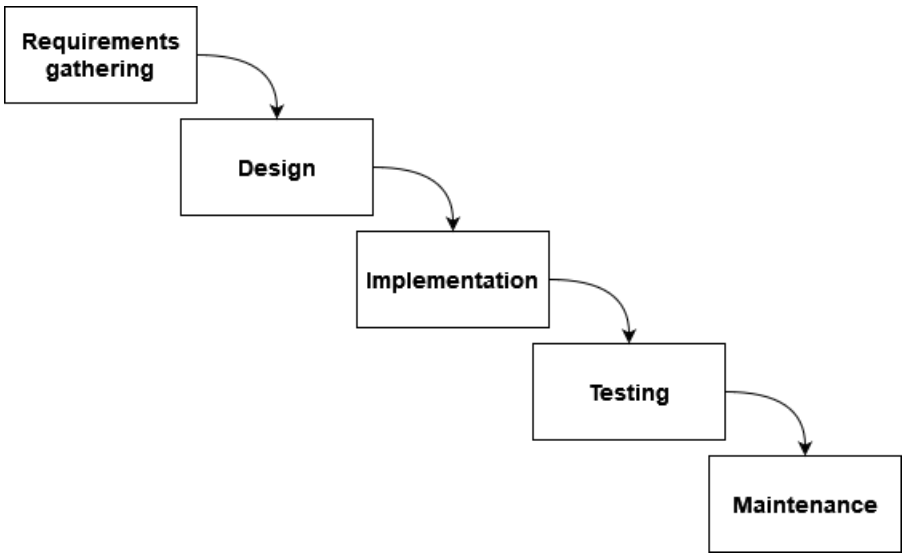


Figure 3.2: Waterfall model

Agile Model

Another well-known model is Agile. It has multiple frameworks, with Scrum and Kanban being the most popular ones. Scrum is a framework where the project is divided into sprints, each lasting between 2-4 weeks, that aim on delivering value to the customer through incremental software features (**scrumban**; **agile**). Kanban focuses on visualizing the project workflow by using a visual board with columns, cards and swimlanes. It uses column limits and a pull system to make the flow of work through the system more efficient (**agile**).

Agile has some drawbacks - its lack of documentation and formal planning, especially in the early stages of the project, may not be suitable for large scale projects (**agile**; **sdlc2**). Similarly, lack of knowledge on how to use the frameworks may be a barrier for some teams (**waterfallno**; **sdlc2**).

Nowadays, the combined use of Scrum and Kanban is becoming quite popular, with many teams employing both frameworks in their projects, allowing them to adopt the appropriate practices and adapt them accordingly based on their needs (**scrumban**).

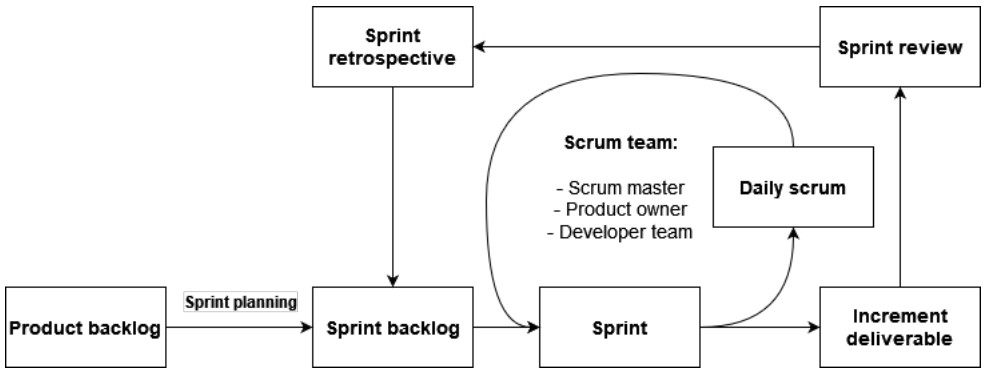


Figure 3.3: Scrum framework

3.1.3 A hybrid approach

A hybrid approach has also been emerging in software development projects. Various surveys report the most common combinations are Scrum, Iterative Development, Kanban, Waterfall and DevOps, with hybrid Waterfall and Scrum being the most popular one (**hybrid1**; **hybrid2**). In this approach, the development part is done in an Agile way, with the rest of the project using Waterfall as a backbone (**hybrid2**).

hybrid1 note that projects using either Agile, traditional or hybrid approach show similar levels of success in terms of budget, time and quality. However, the authors have found

that agile and hybrid approaches perform much better on customer satisfaction than the traditional ones.

3.2 Requirements gathering

Requirements gathering is the first step in any software development process. As described by **reqanalysis2**, a requirement is a 'necessary attribute in a system... that identifies a capability, characteristic, or quality factor of a system in order for it to have value and utility to a user'. Multiple studies mention how proper requirement gathering plays a pivotal role in the project success, with many project failures attributed to poor requirements gathering (**reqanalysis1**; **reqanalysis3**; **reqanalysis5**).

3.2.1 Requirement types

Requirements can be classified into 2 categories: functional and non-functional. Functional requirements describe the system's behavior, while non-functional requirements describe the system's quality attributes, such as performance, security, reliability, etc. (**requirements**).

When writing the requirements in a document, it is important to ensure clarity and conciseness to avoid ambiguity. Based on the recommendations of **requirements** and **requirements2**, the following principles and practices can be followed:

- Write in a simple and consistent language.
- Avoid technical jargon, vague terms, and combining multiple requirements in a single statement.
- Ensure that requirements are necessary, appropriate, complete, feasible, and verifiable.
- Include attributes for each requirement, such as identification, owner, priority, risk, rationale, difficulty, and type (functional/non-functional).

Prioritizing requirements is another crucial task, especially in projects with numerous requirements. Some methods mentioned by **moscow** include using a low to high priority, assigning a numerical value within a specific range or MoSCoW, which classifies requirements into four categories:

- Must have - must be implemented in the software before being released
- Should have - important but not necessary for the software to be released
- Could have - desirable but not necessary for the software to be released
- Won't have - requirements that are not included in the current release

Requirements in Agile

In Agile projects, requirements are written in the form of User Stories, which are simple descriptions of a feature desired by the customer, using a specific format: 'As a [user], I want to [action] so that [benefit]' (**requirements**). Components of a User Story include a title, acceptance criteria, priority, story points and description. Epics are requirements that cannot be completed in a single sprint and can be broken down into user stories. Epics and User Stories are part of the Product and Sprint backlogs, which contain the requirements for the whole project and the current sprint, respectively.

3.2.2 Stakeholders

Stakeholders are the individuals who have some interest in the success of the system or project, thus it is important to identify all possible stakeholders in the early stages of the project to avoid missing important requirements or constraints (**requirements**).

Stakeholder analysis can help understand their position within the project. One way of doing it is by using a stakeholder matrix, such as the Influence/Interest grid (see figure 3.4), which classifies stakeholders based on their influence and interest in the project (**stakeholders**; **stakeholders2**).

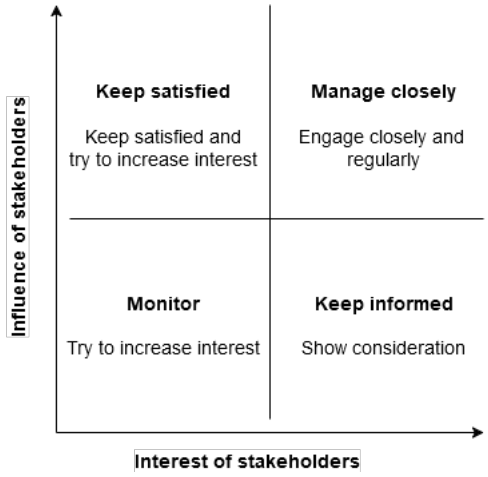


Figure 3.4: Stakeholder Influence/Interest matrix

3.2.3 Requirement gathering techniques

Multiple studies mention the most popular requirement gathering techniques are interviews, workshops, prototyping, modelling, brainstorming, storyboards and observing users

(**reqanalysis1**; **reqanalysis2**; **reqanalysis3**; **reqanalysis4**). In one of them, individuals with multiple years of experience in requirement gathering were interviewed, and the authors found that the most used techniques were collaborative meetings, interviews, ethnography and modelling (**reqanalysis1**).

Multiple research papers recognise interviews as the most common technique for requirement gathering (**interviews5**; **interviews1**; **interviews2**). Some studies have looked at best practices and common mistakes when conducting requirement gathering interviews. The recommended practices, based on **interviews4**; **interviews3**, and the common mistakes, from **interviews1**; **interviews2**, are summarized in Table 3.1 below.

Common Mistakes	**Recommended Practices**
Wrong opening: failing to understand the context before discussing the problem.	State goals at the beginning and allow customer input at the end.
Not leveraging ambiguity to reveal knowledge gaps.	Avoid ambiguity by asking clarifying questions.
Lack of planning: unstructured sequence of questions.	Plan interviews with a structured sequence of questions.
Failing to build rapport with the customer.	Building rapport through small talk or personal questions in the beginning.
Implicit goals: failing to ask or clarify stakeholder goals.	Verify alignment and current interpretation with the customer's vision.
Question omission: not asking about business processes or doing follow-up questions.	Be flexible by probing into relevant topics.
Weak communication: too much technical jargon usage or not listening to the customer.	Use projective techniques like scenarios to encourage deep thinking.
Poor question formulation: vague, technical, irrelevant, or too long.	Break down questions or responses into smaller parts and use story telling.
Wrong closing sequence: skipping interview summaries or feedback.	Leaving time at the end for the stakeholder to offer any feedback or thoughts.

Table 3.1: Comparison of Common Mistakes and Recommended Practices

3.3 Tech stack

3.3.1 Database

There are several types of databases, such as: relational (SQL), NoSQL databases, graph databases or object-oriented databases (**databases2**). The choice of database depends on the project or organisation requirements, such as the amount of data, the complexity of the data, the need for scalability, etc.

Relational databases

Relational databases store structured data in tables, linked through keys to create relationships between entries (**databases**). They use SQL (Structured Query Language) to create queries and schemas to help manage data efficiently. **databases** highlight that relational databases are used, thanks to their high data integrity, for industries like finance and healthcare. Relational databases are widely used, making it easier to find support and resources. However, the rigid schema limits adaptability to rapid data changes or usage of unstructured data. Examples include MySQL, PostgreSQL, Oracle, and Microsoft SQL Server.

NoSQL databases

NoSQL databases manage unstructured or semi-structured data without rigid schemas or relationships (**databases**). As the authors describe, NoSQL databases, such as key-value, document, column-family, and graph databases, excel in flexibility and scalability. NoSQL databases often prioritize performance over strict consistency, making them suitable for large datasets of unstructured data but less ideal for complex transactions. NoSQL systems lack SQL's mature standardization and support. Examples include MongoDB, Cassandra, Couchbase, and Redis.

3.3.2 Backend framework

Choosing the right backend framework is crucial - it is responsible for handling the business logic of the application, such as processing requests, interacting with the database, and returning responses to the client. A good framework also comes with the added benefit of included features such as security and authentication, database support, a big community and documentation.

Based on recent a recent survey by **statista-webframeworks**, the most popular backend frameworks are Express, Flask, Spring Boot, Django and Laravel. This data is also supported by the Stack Overflow Developer Survey 2024, which lists the most popular programming

languages as JavaScript (Express), Python (Flask, Django), Java (Spring Boot) and PHP (Laravel) (**stackoverflow**).

Due to their high popularity among developers, the above frameworks will be compared. Using the information from **spring**; **express**; **django**; **fastapi**, table 3.2 will compare the frameworks based on the following criteria: programming language used, learning curve, community support, security features, database features, and project size suitability.

Framework	**Django**	**FastAPI**	**Spring Boot**	**Express**
Language	Python	Python	Java	JavaScript
Learning curve	Medium	Low	High	Low
Community Support	High	High	High	High
Security features	High	High	High	Medium
Database features	Medium	Low	High	Medium
Project size suitability	Small to medium	Small to medium	Medium to large	Small to medium

Table 3.2: Comparison of backend frameworks

3.3.3 Frontend framework

Similar to the backend frameworks, choosing a suitable frontend framework is equally important - it is responsible for the user interface of the application, such as displaying data, handling user interactions, and making requests to the backend.

Based on the same survey by **statista-webframeworks**, the most popular frontend frameworks are React, Angular, Vue.js, and Svelte. This data is also supported by the Stack Overflow Developer Survey 2024, where those frameworks rank among the highest for desirability and admirability among developers (**stackoverflow**).

Table 3.3 will use the information from **react**; **angular**; **vue**; **svelte** to compare the frameworks based on the following criteria: learning curve, community and documentation, ecosystem and tooling support, performance, state management, and project size suitability.

Framework	**React**	**Angular**	**Vue.js**	**Svelte**
Learning curve	Low	High	Medium	Low
Community and documentation	High	High	High	Medium
Ecosystem and tooling support	High	High	Medium	Low
Performance	High	Medium	Medium	High
State management	High	High	Medium	Low
Project size suitability	Small to large	Medium to large	Small to medium	Small to medium

Table 3.3: Comparison of frontend frameworks

3.4 Large Language Models (LLMs)

Large language models (LLMs) are artificial intelligence systems that are used for natural language processing (NLP) tasks such as text generation, translation, summarization and question answering (**llm2**; **llm_healthcare**). Additionally, LLMs have been found to have emergent capabilities, like reasoning, planning, decision-making and in-contenxt learning (**llm2**). These extraordinary capabilities are achieved through extensive training on large corpus of text data, high parameter count (in the billions) and usage of techniques such as fine-tuning or prompt engineering to improve their performance (**llm2**; **llm_healthcare**).

LLMs are built on the transformer architecture, which allows them to understand text by learning and remembering the relationships between words (**llm**). These models are first pre-trained on large amounts of unlabeled data using, allowing them to excel in a wide variety of tasks (**foundation**; **llm2**). These pre-trained models, known as foundation models such as the GPT or Llama families, can then be fine-tuned for specific tasks, improving their performance and accuracy even further (**gpt4**; **llama3**; **llm2**).

3.4.1 Multimodal LLMs

One advancement in the field of LLMs has been the addition of multimodal abilities, allowing them to process, understand and generate text and images, audio or videos (**mllm**; **mllm2**). These new multimodal LLMs (MLLMs) utilise existing reasoning capabilities of LLMs, which are connected to an encoder that can processes images, audio or videos and a generator that helps with generating multimodal outputs (**mllm**). This integration of new modalities allows MLLMs to become versatile tools, expanding their possible use cases and bridging the gap between human and machine interaction (**llm_healthcare**).

API model providers

Running and hosting LLMs locally can be a challenge, considering their big model sizes and high computational requirements. As such, many platforms offer APIs that allow users to access LLMs through the cloud. A list of some free API providers, the models offered and their rate limits has been compiled by **llmapi** and some are listed in the table below.

Provider	**Model name(s)**	**Free tier limits**
Groq	Llama 3.2 11B Vision	7,000 requests/day, 7,000 tokens/minute
	Llama 3.2 90B Vision	3,500 requests/day, 7,000 tokens/minute
OpenRouter	Llama 3.2 11B Vision Instruct Llama 3.2 90B Vision Instruct Gemini 2.0 Flash Experimental	20 requests/minute, 200 requests/day
Google AI Studio	Gemini 2.0 Flash	4,000,000 tokens/minute, 10 requests/minute
	Gemini 1.5 Flash	1,000,000 tokens/minute, 1,500 requests/day, 15 requests/minute
	Gemini 1.5 Pro	32,000 tokens/minute, 50 requests/day, 2 requests/minute
GitHub Models	OpenAI GPT-4o OpenAI GPT-4o mini	Rate limits dependent on Copilot subscription tier
Cloudflare Workers AI	Llama 3.2 11B Vision Instruct	10,000 tokens/day
glhf.chat	Any model on Hugging Face that fits on an A100 node (640GB VRAM)	480 requests/8 hours

Table 3.4: API providers for LLMs

3.4.2 LLMs in healthcare

One application of MLLMs is in healthcare, where the growing volume and complexity of data creates the need for more advanced tools to process and analyze it. LLMs and MLLMs have found use in various healthcare applications, either by using existing models or by developing new, specialized medical models such as Med-PaLm2, BioMistral or Med-Gemini (**biomistral**; **medgemini**; **medpalm2**). Some of these applications include:

- **Improving medical diagnosis:** By combining patient records, existing symptoms, and medical history, LLMs can use their reasoning capabilities and memory to assist in diagnosing or preventing health conditions (**llm_healthcare**; **llm_healthcare3**; **llm_healthcare4**).
- **Medical Imaging and Multimodal Capabilities:** In diagnostic imaging, multimodal models can assess both text and images (such as X-rays and MRIs) to offer comprehensive analysis. Clinicians can input medical images and contextual information, making MLLMs valuable assistants in the real-time diagnostic processes (**llm_healthcare3**).
- **Virtual Health Assistants:** LLMs can also be deployed as virtual assistants, helping patients with personalised care and general health inquiries (**llm_healthcare**; **llm_healthcare3**). Patients in areas with limited healthcare access can benefit from these assistants, which also supports healthcare providers by lightening their workloads.
- **Administrative Support:** LLMs can assist in generating Electronic Health Records (EHRs), allowing healthcare providers to focus more on patient interaction (**llm_healthcare4**). Additionally, they can also help translate complex medical terms into more simple language, assist in administrative tasks, and more.

3.4.3 Prompt Engineering

The success of LLMs depends not only on the model itself - but also on how it's effectively used by the users, using techniques like prompt engineering, which involves the constant designing and refining of prompts to guide the output of LLMs (**promptmed**; **prompt2**). Prompts represent instructions given to the model to guide its output, such as providing context, examples, or constraints to the model (**prompt**; **prompt1**; **prompt2**).

There are multiple techniques for prompt engineering, ranging from simple to more advanced. The tables and subsections below outlines some of the most common techniques.

Zero-Shot Prompting

Zero-shot prompting are techniques where the LLM is given a prompt without any examples, allowing it to generate an output based on the prompt alone (**prompt1**).

Technique	Description	Source
Role prompting	Assigning a specific role to the LLM in the prompt. The authors note that generally it provides mixed results but may be useful in certain settings.	**role1**
Style prompting	Specifying the desired style or tone in the prompt.	**style**
Emotion prompting	Incorporating phrases of psychological relevance to humans in the prompt.	**emotion**
Re-reading	Adding the phrase 'Read the question again' to the prompt in addition to repeating the question.	**rereading**
Self-Ask	Prompting the LLM to decide if it needs to ask any follow-up questions for a given prompt.	**selfask**

Table 3.5: Zero-Shot Prompt Techniques

Few-Shot Prompting

Few-shot prompting are techniques where the LLM learns how to complete a task based on a few examples given in the input prompt (**prompt1**).

Technique	Description	Source
Self-Generated In-Context Learning	Using the LLM to automatically generate examples when training/example data is not avaialable.	**self-generating**
Prompt Mining	Scanning the training data to discover common formats that can be used as prompt templates.	**mining**

Table 3.6: Few-Shot Prompt Techniques

Thought Generation Prompting

Thought generation are techniques where the prompt encourages the LLM to explain its reasoning process while solving a given problem (**prompt1**).

Technique	Description	Source
Chain-of-Thought (CoT)	Adding a phrase like 'Let's think step by step' at the end of the prompt to encourage the LLM to describe its thought process before offering a final answer.	**cot**
Contrastive CoT	Using CoT and also adding both incorrect and correct examples in order to provide the LLM a more diverse example set.	**contrastive-cot**
Auto-CoT	Using CoT with another LLM to automatically generate CoT examples that can be used to create few-shot CoT prompts for other LLMs.	**auto-cot**
Least-to-Most	Starts with asking the model to break down a problem into sub-problems without solving them. Afterwards, it solves them one by one, appending the result each time, until it arrives at the answer.	**least-most**
Tree-of-Thought (ToT)	Starts with an initial problem and then generates multiple possible steps by using CoT. Then, it evaluates each step, decides which one to take and creates more thoughts until it reaches an answer.	**treeofthought**

Table 3.7: Thought Generation Prompt Techniques

Multimodal and Multilingual Prompting

Multimodal and multilingual prompting are techniques which aim to improve an LLM's performance by leveraging multiple modalities or languages in the prompt (**prompt1**).

Technique	Description	Source
Translate-first prompting	Translating the input prompt into English to leverage LLMs strengths in dealing with English inputs, compared to non-English inputs.	**translate-first**
English prompting	Writing the prompt in English may usually be more effective than using the task language for multilingual tasks. The authors argue it may because of the predominance of the English language in the pretraining data.	**english-prompting**
JSON/XML output formatting	Asking the LLM to format the response in a JSON or XML format and providing the expected schema has been found to improve the accuracy of LLM outputs	**jsonllm**
Multimodal CoT	Similar to the textual CoT, this technique encourages the model to solve a given image-based problem step by step by step.	**multimodal-cot**
Image-as-Text	Generating or writing a textual description of an image that can then be included in a text-based prompt.	**images-as-text**
Chain-of-Images (CoI)	Using the CoT process to generate images as part of its thought process to reason visually.	**coi**

Table 3.8: Multimodal and Multilingual Techniques

Agents

Agents are techniques which encourage LLMs to use external tools or resources to complete a task (**prompt1**).

Technique	Description	Source
Program-aided Language Model (PAL)	Using the LLM to translate a problem into code, which can then be sent to an interpreter to generate an answer.	**pal**
ReAct	Firstly, the model generates a thought based on the input. Then, the model takes an action and observes the result. This process is repeated until the model arrives at an answer.	**react-llm**
Retrieval Augmented Generation (RAG)	This technique involves retrieval of information from an external source and inserting it into the prompt.	**rag**

Table 3.9: LLM Agent Techniques

3.4.4 Challenges and concerns of using LLMs

While LLMs bring many benefits when applied to the healthcare domain, it is important to note that their use does come with several challenges:

- **Data Privacy and Compliance:** Patient data is highly sensitive, thus ensuring compliance with standards is essential, requiring data anonymization and secure handling practices to ensure patient data safety.(**llm_healthcare**; **llm_healthcare2**; **llm_healthcare4**).
- **Transparency and Explainability:** LLMs are often described as 'black boxes', making it difficult to explain their decision-making processes. In healthcare, transparency is crucial - lack of it poses risks and raises ethical concerns about relying on such systems in high-stakes scenarios (**llm_healthcare**; **llm_healthcare2**; **llm_healthcare4**)..
- **Bias and Fairness:** LLMs trained on vast datasets can inherit biases in the data, leading to skewed or unfair outcomes (**llm_healthcare2**).
- **Hallucinations:** LLMs sometimes generate false or fabricated outputs, also known as 'hallucinations'. In healthcare, this poses significant risks, as incorrect or misleading information could jeopardize patient safety and trust in the technology (**llm_healthcare4**; **llm_healthcare**).
- **Accountability:** Responsibility must be clearly communicated and understood by all parties involved in the development and use of the model (**llm_healthcare2**). The author recommends the usage of clear guidelines, policies and code of conducts

to ensure that all parties are aware of their obligations.

- **High Costs and Infrastructure Needs:** Training and operating LLMs requires extensive computational resources, which can be a limiting factor for healthcare institutions (**llm_healthcare4**).

3.5 PHR Systems

A Personal Health Record (PHR) is an electronic resource used by patients to manage their own health information (**phrsecurity**; **phrlist**). PHRs are different from Electronic Health Records (EHRs) and Electronic Medical Records (EMRs) which are inter-organisational or internal systems to organise patient health records (**phrdiff**; **phrlist**). Three different types of PHRs are described by **phrsecurity**: stand-alone, which require manual entry to update the records; instituion-specific, which are connected to a specific healthcare institution; and integrated, which can connect to multiple healthcare systems to aggregate data from multiple sources.

Usage of PHRs can bring many benefits to patients, such as: empowering patients to manage their health, improving patient outcomes, decreasing the cost of healthcare and improving the taking of medication (**phrsecurity**).

PHRs contain highly sensitive health information, so it is important to ensure that the data is secure and private. Based on a survey of health information management and medical informatics experts, **phrsecurity** identified 7 dimensions that need to be addressed when developing a PHR system:

1. Confidentiality
2. Availability
3. Integrity
4. Authentication
5. Authorization
6. Non-repudiation
7. Access rights

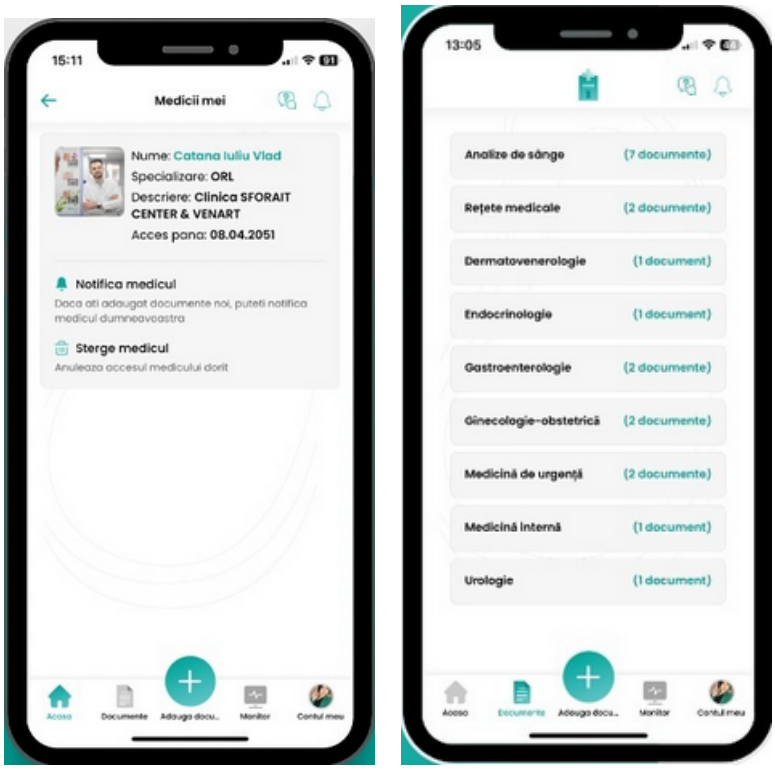
The authors recommend mechanisms to ensure adherence to the above-mentioned dimensions, such as encrypting the data in the database, using backups or defining user access to data and access rights.

3.5.1 Existing Solutions

PHR systems have been implemented nation-wide in many developed countries, such as the NHS App in the UK (**phrlist**). Additionally, there are many private solutions that offer similar features to the one proposed in this project. The next sections will provide a brief overview of 3 existing systems: Medvalet, Andaman7 and Fasten Health.

Medvalet

A mobile app developed in Romania that allows patients to upload their medical history as PDFs or scanned documents (**medvalet**). See Table 3.10 for a summary of its features and limitations and figure 3.5 for a screenshot of the app.



(a) My doctors screen (b) Uploaded documents screen

Figure 3.5: Medvalet screenshots

Key Features/Benefits	Limitations/Drawbacks
• Upload medical history as PDFs or scanned documents. • Categorize documents by type (e.g., prescriptions, lab results). • Graphically track vitals like blood pressure and weight over time. • Patients can input personal details such as name, age, and weight. • Doctors can access patient history directly via the app.	• Requires doctors to create accounts, which may deter use. • Doctors can access patient history without explicit consent, raising privacy concerns. • App acts as document storage, which can be cumbersome to access for lengthy histories. • Lacks data extraction or summarization features from uploaded documents. • Only available as a mobile app, limiting accessibility for desktop-only users.

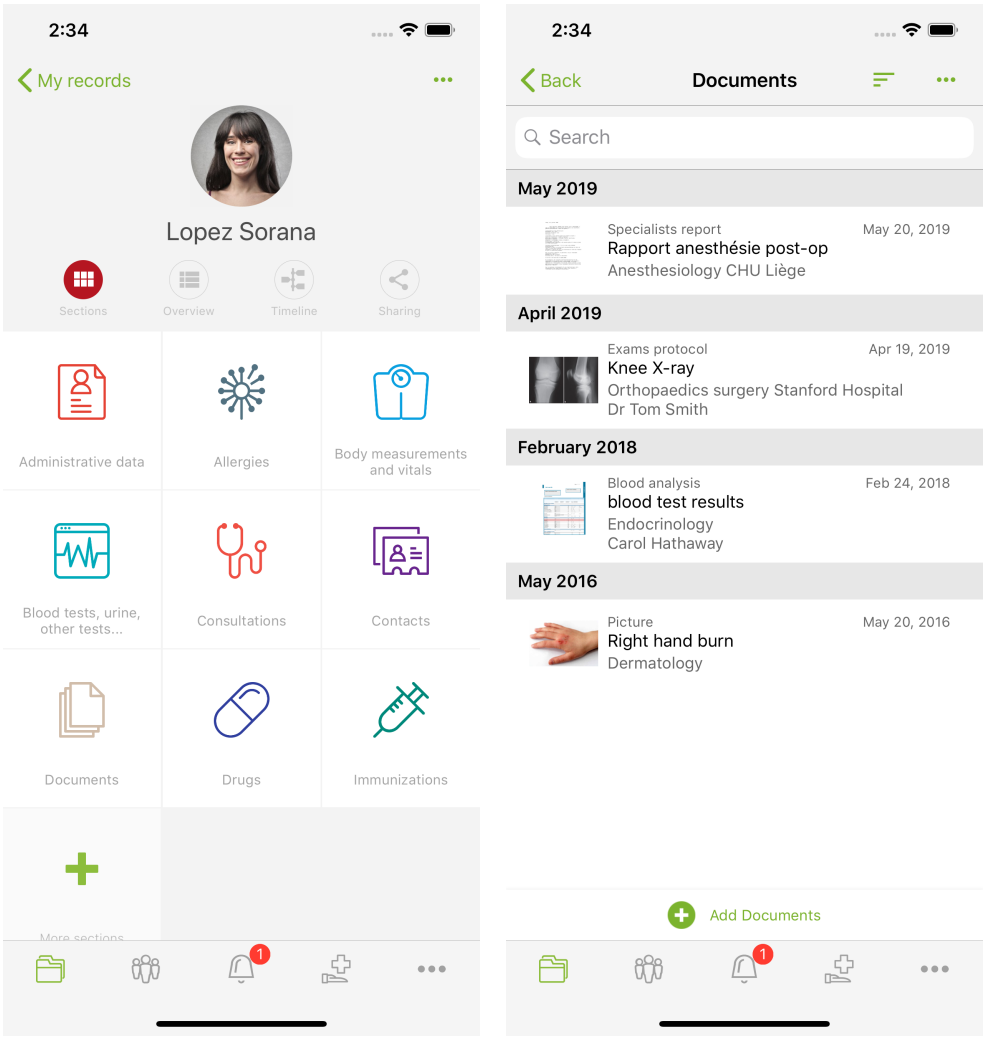
Table 3.10: Medvalet Features and Limitations

Andaman7

A mobile app developed by a Belgian-American eHealth company with the goal to improve doctor-patient communication, compliant with GDPR and HIPAA (**andaman**). See Table 3.11 for a summary of its features and limitations and figure 3.6 for a screenshot of the app.

Key Features/Benefits	Limitations/Drawbacks
• Offers sections for personal information, medical history, allergies, vaccinations, medications, etc. • Automatically collects health data from over 300 hospitals and clinics in the US and Europe. • Supports input from diverse sources like hospitals, labs, smart devices or even manual input. • Stores data locally on patients' devices, ensuring privacy. • Data sharing with QR codes and revokable access. • AI tools for summarization, translation, and simplifying medical jargon.	• Requires patients and doctors to both create accounts. • Does not extract data or values from uploaded documents like lab results. • Limited to mobile platforms, which may limit usability for desktop-only users.

Table 3.11: Andaman7 Features and Limitations



(a) PHR Sections screen

(b) Documents section screen

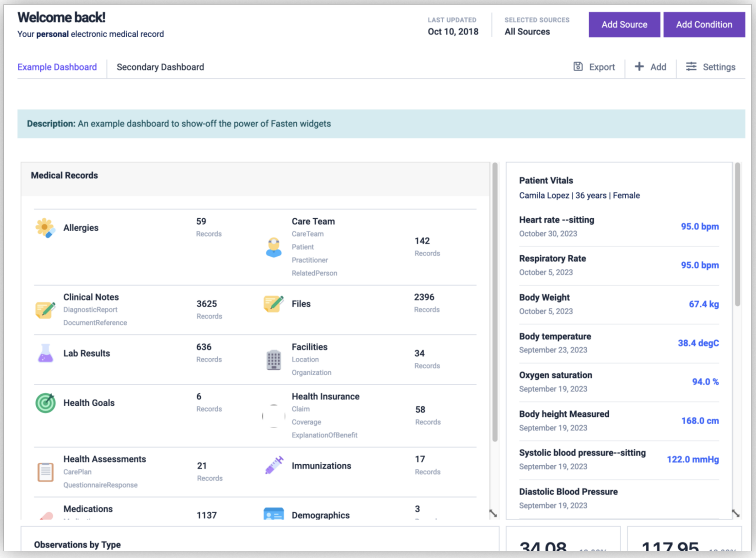
Figure 3.6: Andaman7 screenshots

Fasten Health

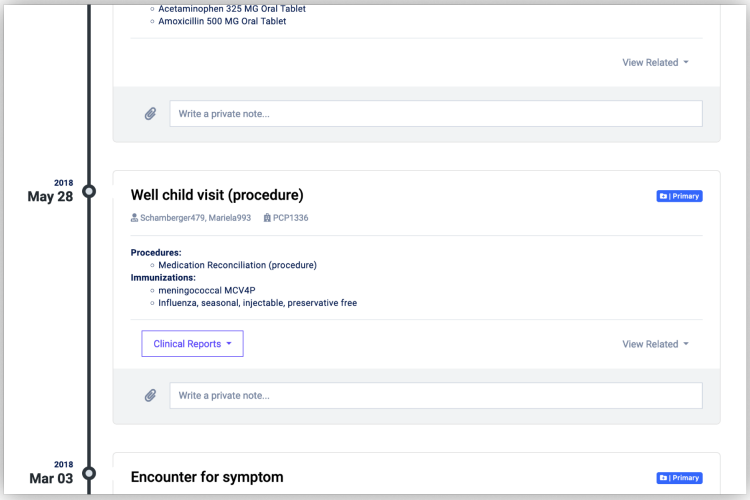
An open-source, self-hosted electronic medical record aggregator with optional paid desktop versions for Windows and Mac (**fasten**). See Table 3.12 for a summary of its features and limitations and figure 3.7 for a screenshot of the app.

Key Features/Benefits	**Limitations/Drawbacks**
• Automatically aggregates records from multiple providers, like hospitals and labs. • Supports self-hosting for complete control over data, stored locally. • Compatible with protocols such as DICOM, FHIR, and OAuth2. • Allows manual entry for allergies, vaccinations, and medications. • Offers multiple dashboards with graphs to visualize health data. • Supports multi-user functionality for families.	• Paid desktop versions may deter users. • Manual data entry limited to new or existing encounters, complicating usage. • Does not support OCR or automatic data extraction from documents. • Lacks data-sharing capabilities with doctors. • Requires technical expertise for self-hosting. • Restricted to healthcare providers in the United States.

Table 3.12: Fasten Health Features and Limitations



(a) Dashboard screen



(b) Visit history screen

Figure 3.7: Fasten Health screenshots

Chapter 4

Project Planning and Design

4.1 UML Diagrams

UML, or Unified Modeling Language, is a standardized modeling language that consists of a set of diagrams used for modeling business processes and documenting software systems, helping better communicating potential designs and architectural decisions (**uml**).

The most common UML diagrams include:

- **Use Case Diagram** - Illustrates the system's intended functionality in terms of actors, use cases, and their relationships, showing how the system delivers value to users. The diagram can also be accompanied by a use case specifications document, which provides a detailed description of each use case.
- **Class Diagram** - Depicts the structure of the system by showing classes, attributes, operations, and static relationships between classes.
- **Sequence Diagram** - Demonstrates how objects interact in a particular, timed sequence scenario, focusing on the messages passed between objects.
- **Activity Diagram** - Represents the workflow of a target use case or business process through a series of activities, emphasizing steps, choices, iterations, and concurrency.

The student has used UML diagrams to present the stakeholders with a visual representation of the system's design and functionalities. The diagrams can be found below, under their respective sections.

4.1.1 Use Case Diagram

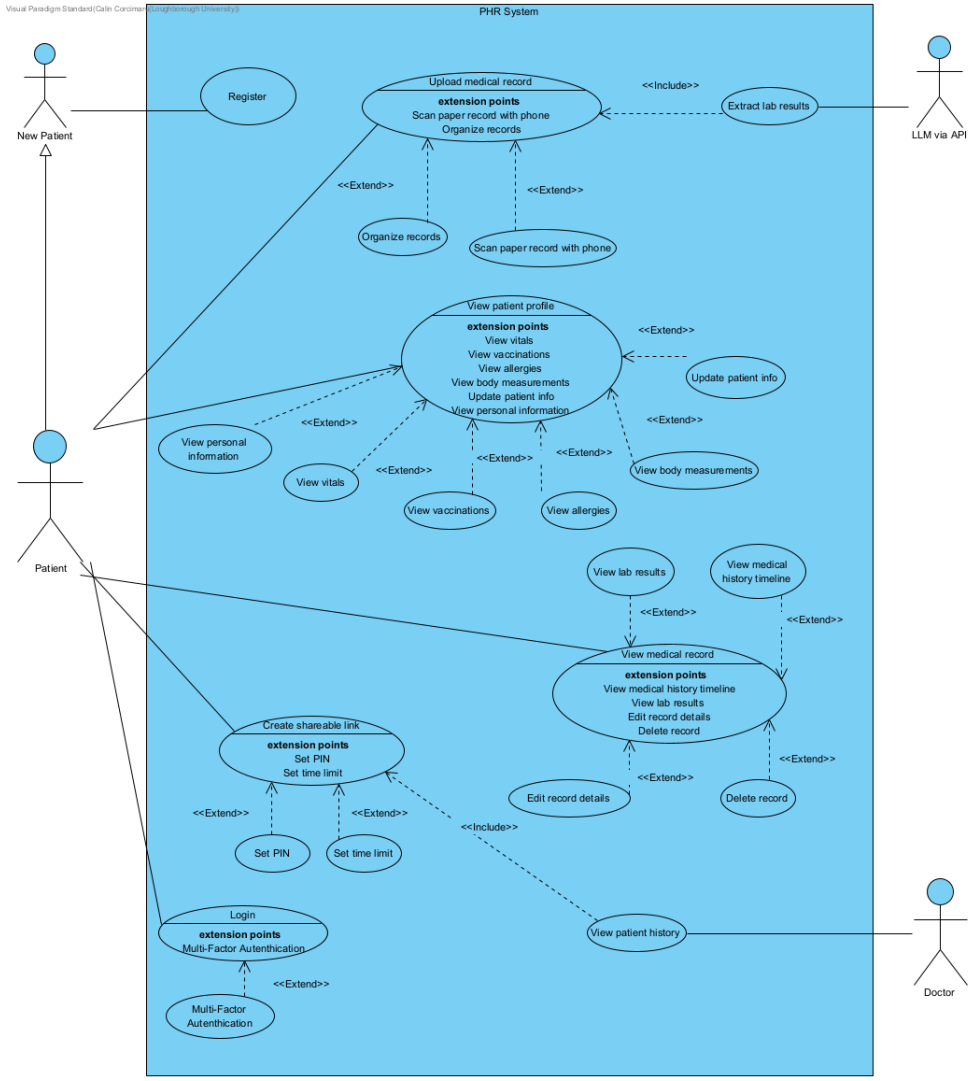


Figure 4.1: UML Use Case Diagram

4.1.2 Use Case Specifications

Login

Description	The Login use case allows the app user to log in to their existing account via their credentials, with an optional use of MFA.
Actors	Patient
Preconditions	Must have an existing account
Steps	1. User enters user and password 2. User clicks on the login button 3. App validates user credentials 4. Patient enters MFA code if enabled 5. App logs user in

Register

Description	The Register use case allows the app user to create a new account.
Actors	New Patient
Preconditions	No existing account with the email used to register
Steps	1. User enters user and password 2. User clicks on the register button 3. App validates user credentials 4. App logs user in 5. App sends verification email 6. User verifies email

Upload Record

Description	The Upload Record use case allows the patient to upload their medical records to the app.
Actors	Patient, LLM
Preconditions	Must be logged in
Steps	1. User selects file upload (or camera scan) 2. User selects the record to upload 3. User clicks on the upload button 4. App validates the record 5. User selects the appropriate record type 6. If record type is lab result, app sends the record to LLM via API for processing into JSON format 7. App adds the record to the database 8. App shows confirmation to user

Share Records

Description	The Share Records use case allows the patient to share their medical records with doctors.
Actors	Patient, Doctor
Preconditions	Must be logged in and have records uploaded
Steps	1. User selects option to create a share link 2. OPTIONAL: User selects the records to share 3. OPTIONAL: User adds a PIN to the share link 4. User selects time limit for the share link 5. App generates the share link 6. App sends the share link to the doctor via email 7. App shows confirmation to user 8. Doctor clicks on the share link 9. Doctor enters the PIN (if required) 10. App validates the PIN 11. App shows the records to the doctor

View Records

Description	The View Records use case allows the patient to view and edit their uploaded medical records.
Actors	Patient
Preconditions	Must be logged in and have records uploaded
Steps	1. App provides a list of records or medical history 2. User selects record to view from list or medical history 3. App retrieves the record from the database 4. App shows the record to the user 5. OPTIONAL: User can view the record in a graphical format if lab result 6. OPTIONAL: User edits the record 7. OPTIONAL: User deletes the record

View Patient Profile

Description	The View Patient Profile use case allows the patient to view and edit their profile information, including health information such as allergies, medications, vaccinations and recorded health data like blood pressure, glucose levels, etc.
Actors	Patient
Preconditions	Must be logged in
Steps	1. User selects the profile section 2. App retrieves the profile information from the database 3. App shows the profile information to the user - vaccinations, allergies, medications, health data 4. OPTIONAL: User edits the profile information 5. OPTIONAL: User adds new health data 6. OPTIONAL: User deletes health data 7. OPTIONAL: User can view health data in a graphical format

4.1.3 Class Diagram

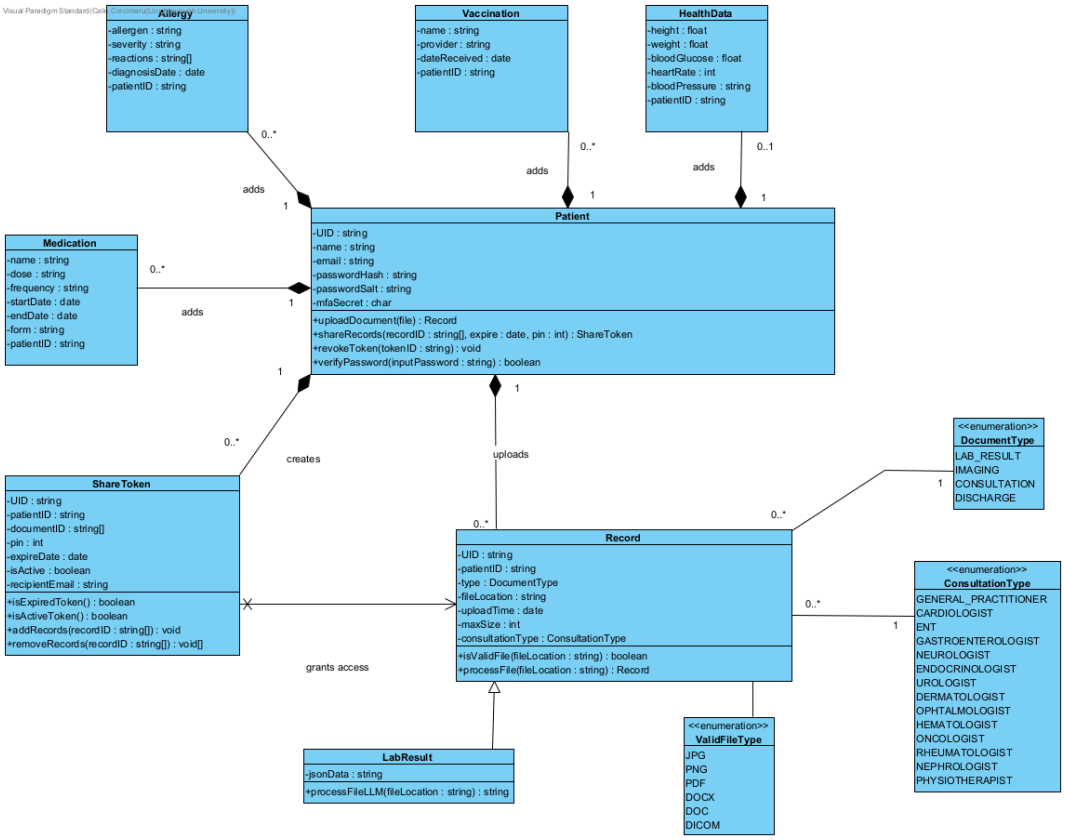


Figure 4.2: UML Class Diagram

4.1.4 Sequence Diagrams

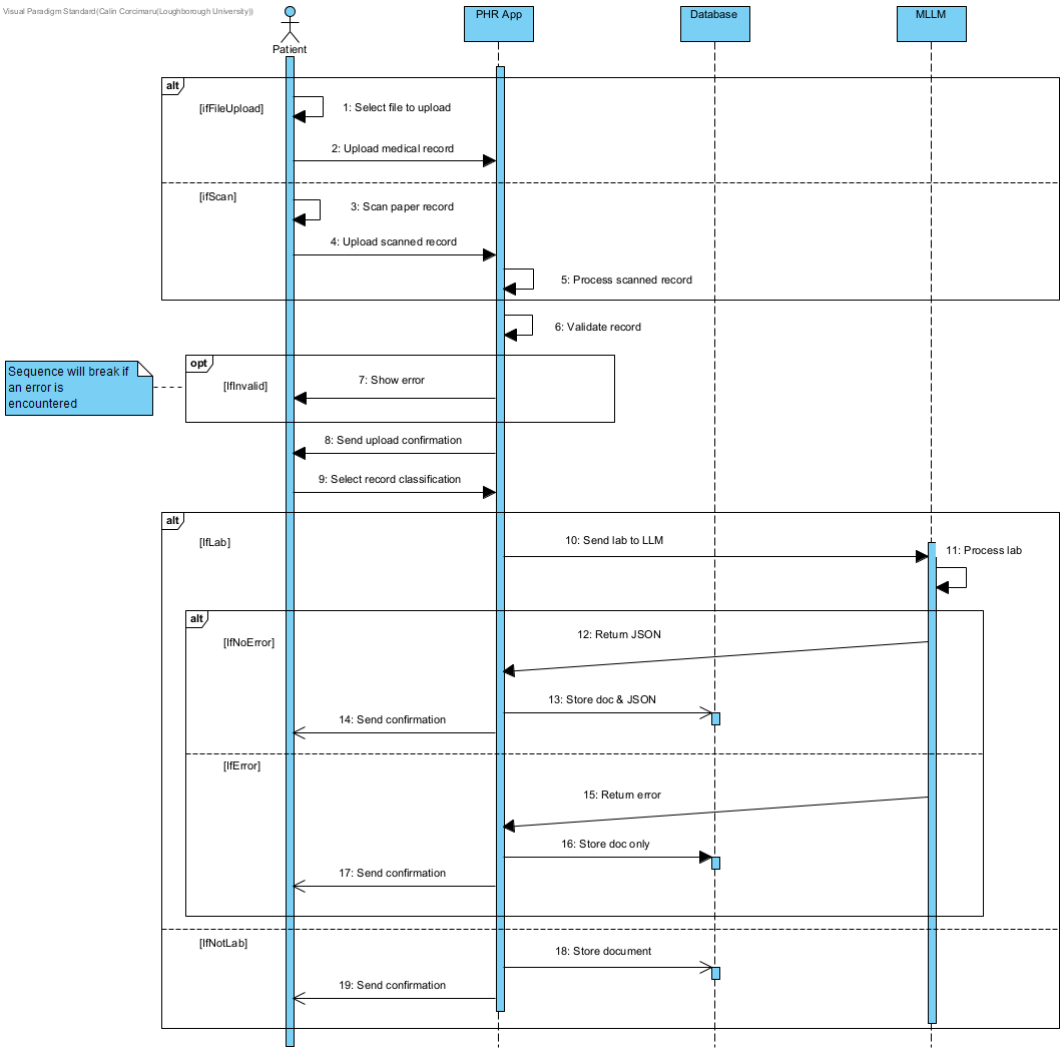


Figure 4.3: UML Sequence Diagram - Upload Record Use Case

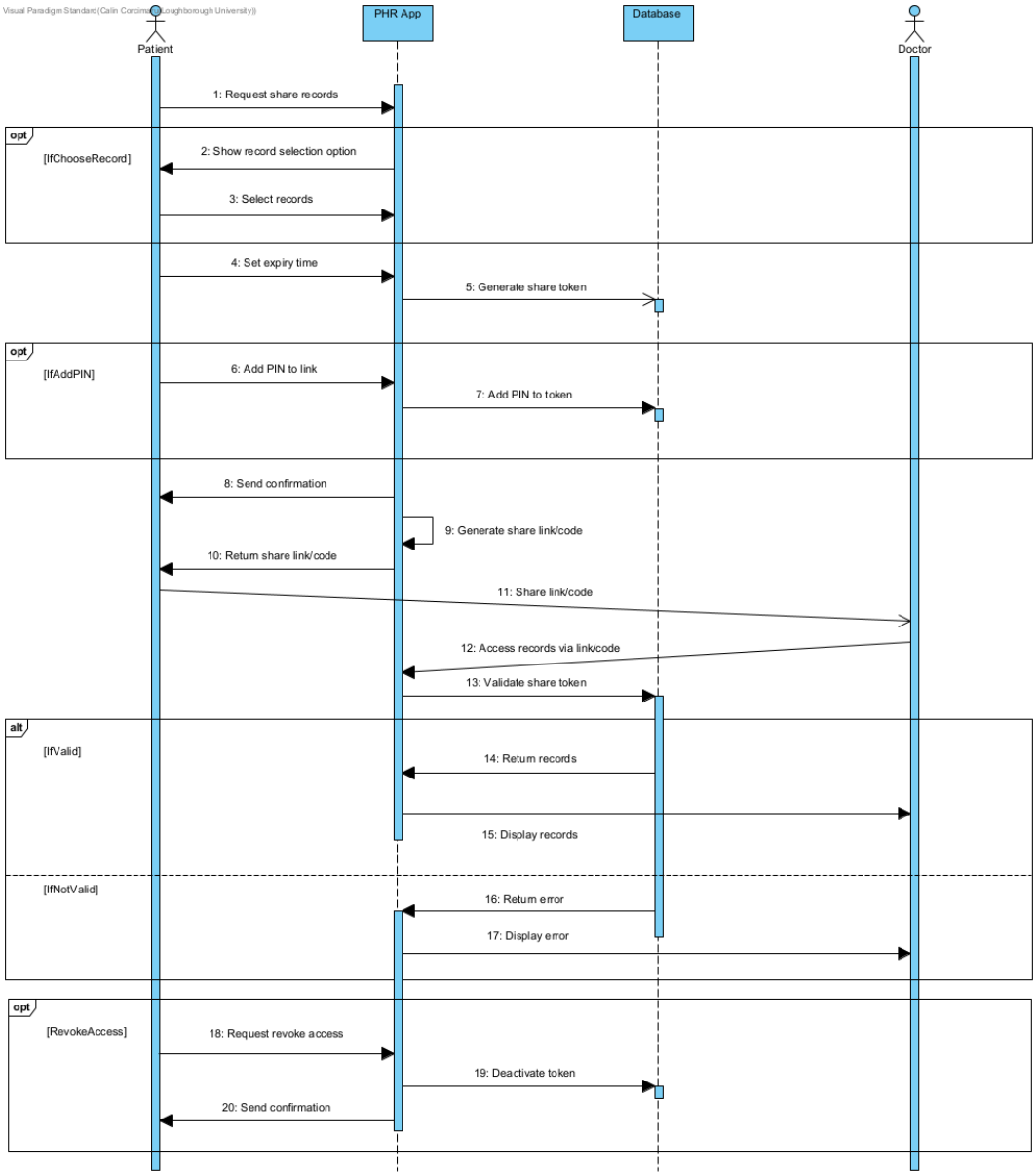


Figure 4.4: UML Sequence Diagram - Share Records Use Case

4.1.5 Activity Diagrams

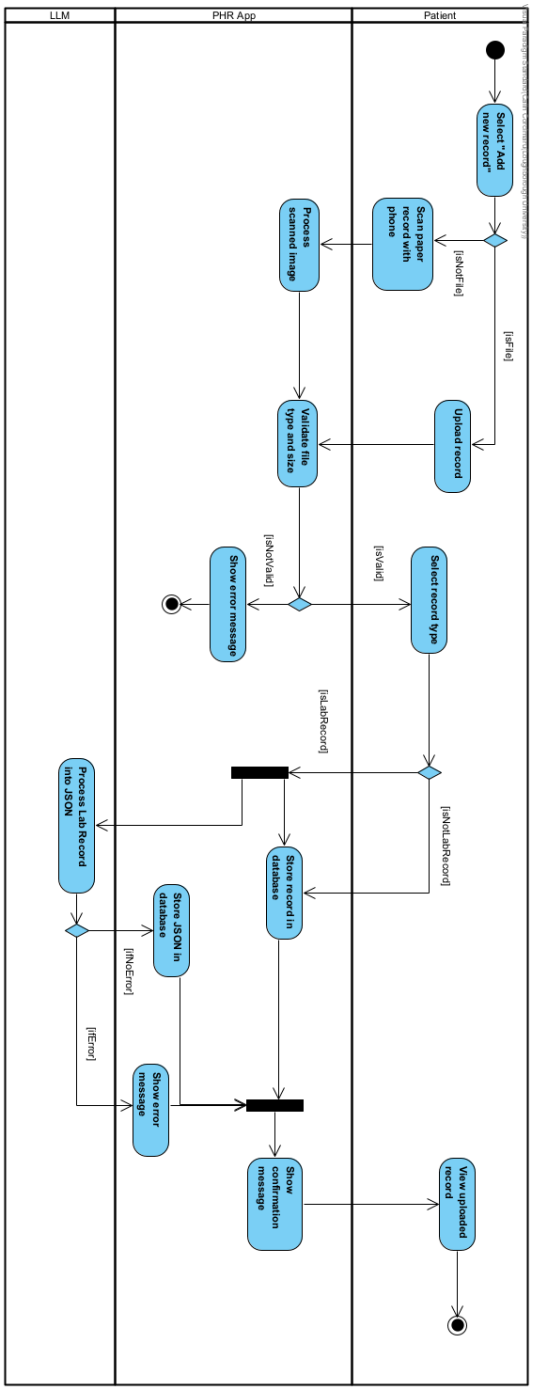


Figure 4.5: UML Activity Diagram - Upload Record Use Case

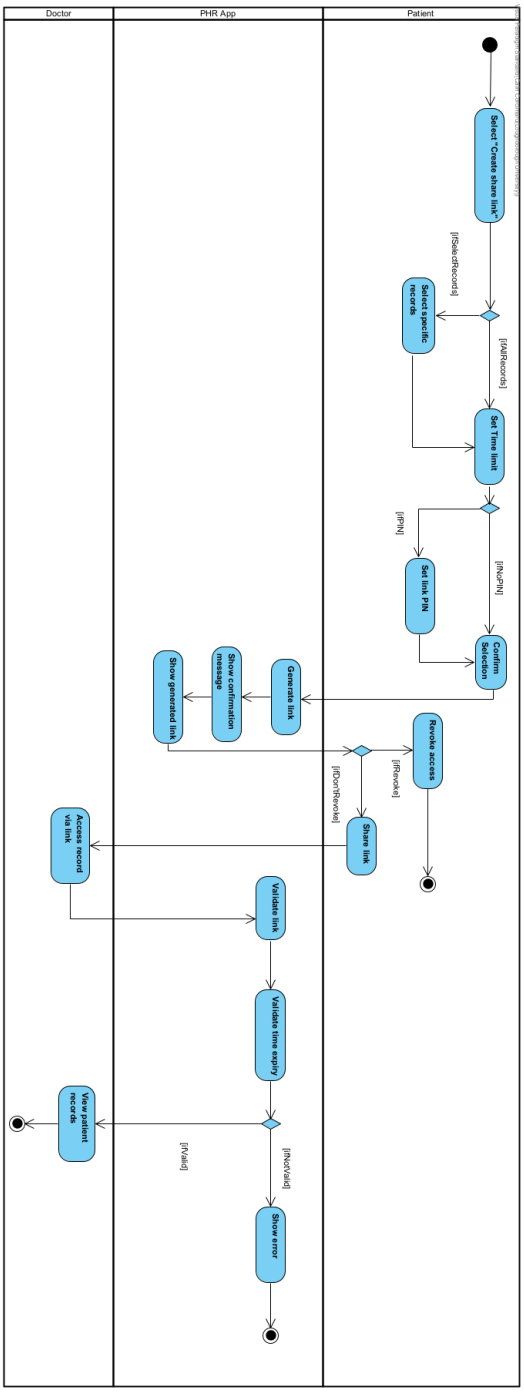


Figure 4.6: UML Activity Diagram - Share Records Use Case

4.2 Database Design

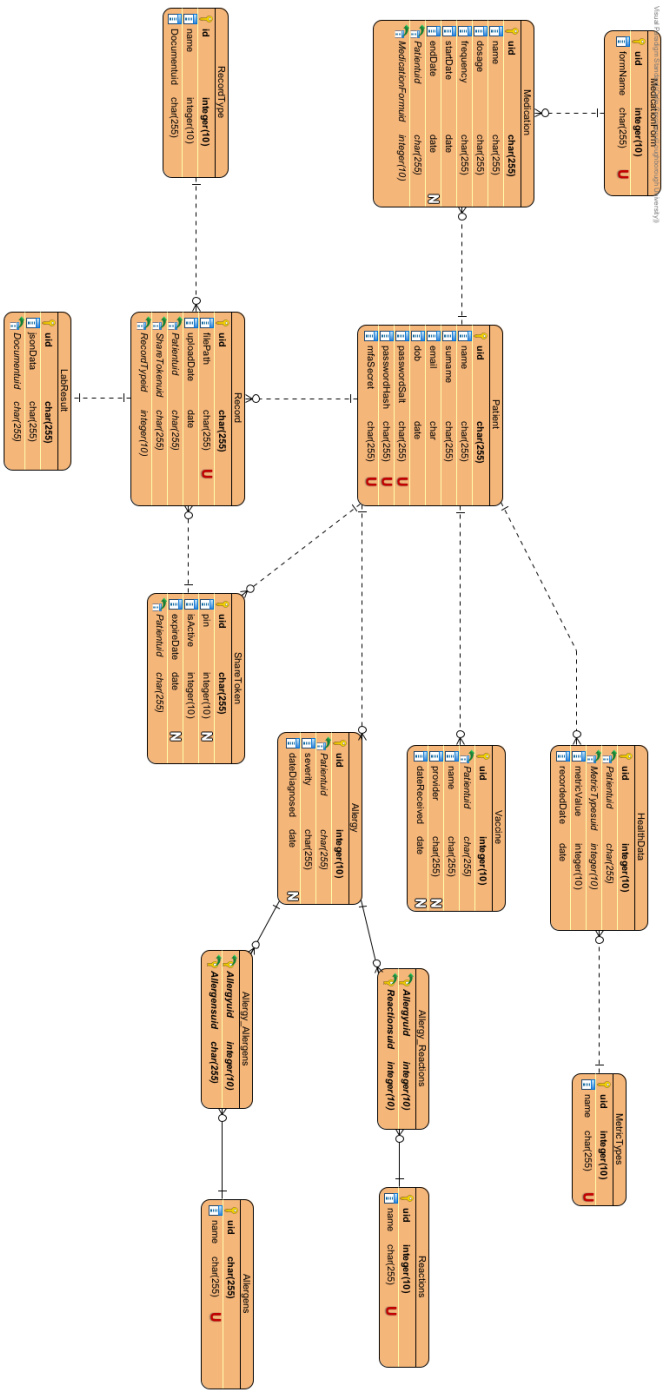


Figure 4.7: Entity Relationship Diagram

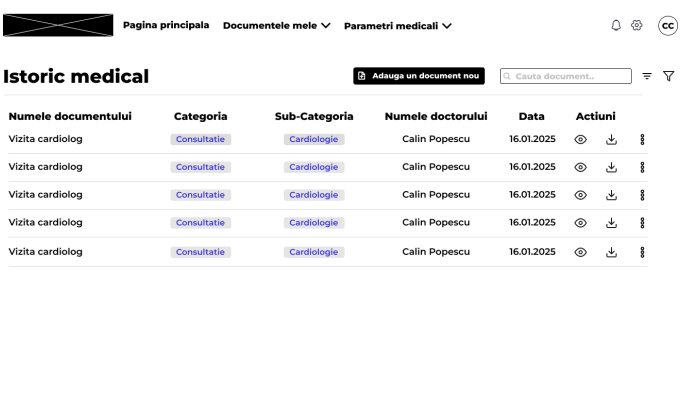
4.3 Wireframes

Wireframes have been used to provide a high-level overview of how the web application would look like and present some of its key functionalities. The wireframes have been created using Figma and then shown to some of the stakeholders to gather feedback. Based on the feedback received, the wireframes have been adjusted and some examples can be seen below in figures 4.8, 4.9 and 4.10 while the full set of wireframes can be found in the appendix B.

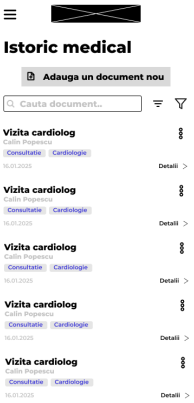
(a) Desktop version

(b) Mobile version

Figure 4.8: Desktop and Mobile version of the Dashboard screen

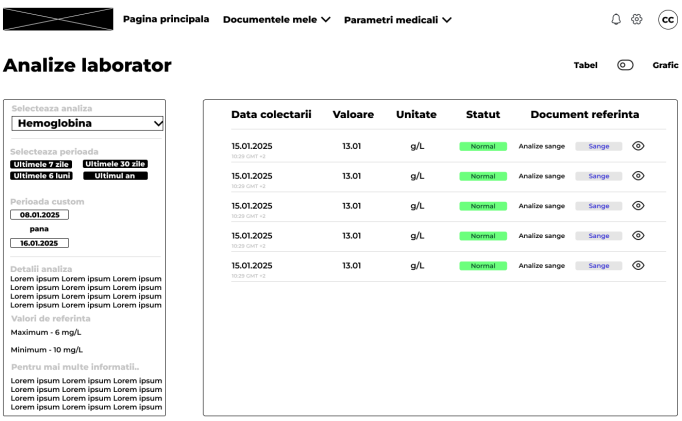


(a) Desktop version



(b) Mobile version

Figure 4.9: Desktop and Mobile version of the Medical History screen



(a) Desktop version

(b) Mobile version

Figure 4.10: Desktop and Mobile version of the Lab Test Results screen

4.4 Project Tech Stack

Based on the research conducted in sections 3.3.1, 3.3.2 and 3.3.3, the student has decided to use the following technologies for the project, which are shown in the diagram 4.11 below.

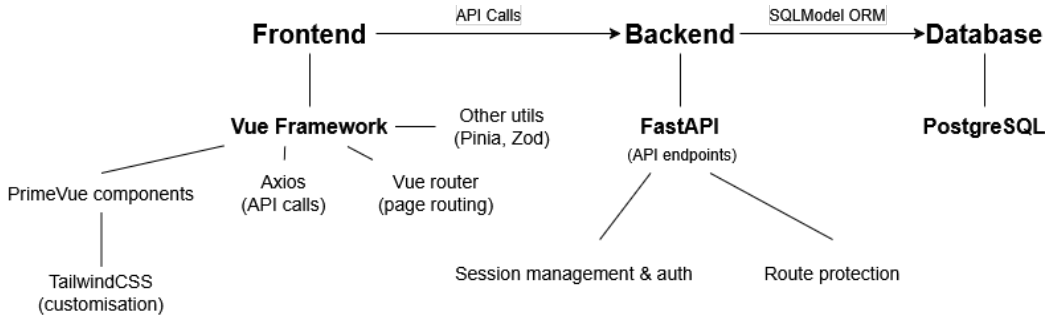


Figure 4.11: Proposed System Architecture

In the next subsections, each part of the system will be discussed in more detail.

4.4.1 Frontend

For the frontend part of the project, the student has decided to use Vue, which is a JavaScript framework for building single-page applications (SPAs) and UIs (**vue**). This framework's strengths lie in its ease of use and flexibility, with features like component and view-based architecture, element reactivity and Single File Components (SFCs) that allows HTML, CSS and JavaScript to be combined in a single `.vue` file. Vue also boasts a large and active community, with many libaries and guides available for developers. Finally, the student has had previous experience working with Vue in their Team Project module, making it an ideal choice for this project.

Diagram 4.12 below showcases how different components and libraries of the frontend will interact with each other. The next subsections will discuss each part in more detail.

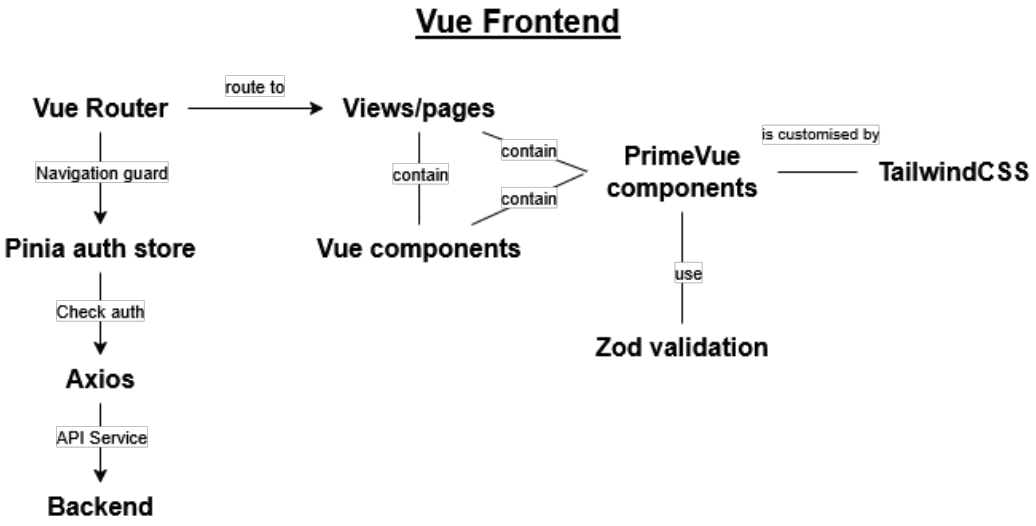


Figure 4.12: Interaction of Frontend Components

Vue Router

One of the key elements of the frontend is the Vue Router. It is the official client-side router for Vue.js, which allows the user to navigate between different pages of the application without a full page reload (**vuerouter**). This makes the full use of the SPA capabilities of Vue, providing a seamless and fast user experience. Similarly, Vue Router can be used to create navigation guards to protect certain routes from unauthorized access, which is crucial for the security of the application.

Pinia

The next element is Pinia, which is a store library for Vue made by the same team that created the frontend framework (**pinia**). Its main functionality is to provide a way to share states across Vue components and pages. In this project, Pinia can be used to store the user's authentication status and other global states that need to be shared across the application.

Axios

The next element is Axios, which is a promise-based HTTP client for the browser and Node.js (**axios**). It is used to make HTTP requests to the backend API, which is crucial for the frontend to interact with the backend. Similarly, it allows for the automatic interaction with cookies in the requests sent and responses received, which is important for the authentication process.

Vue views and components

Vue components and views (or pages) represent the foundation of the frontend for the application. Components allow to break down the UI into smaller, independent and reusable elements, which can be later combined to create the frontend of the application (**vuecomponents**). Each component can be stored in a separate `.vue` file and then imported within a view/-page or another component. Views, on the other hand, represent the different pages of the application, which can be navigated to using the Vue Router.

PrimeVue and TailwindCSS

The final two elements of the frontend are PrimeVue and TailwindCSS. PrimeVue is a component library for Vue, which provides a set of pre-built components that can be used to more easily create the frontend of the application (**primevue**). TailwindCSS, on the other hand, is a CSS framework that provides a set of utility classes that can be used to style the different elements of the application (**tailwind**). In this application, PrimeVue provides the basic components like buttons, forms, and tables, while TailwindCSS is used to style these components.

4.4.2 Backend

For the backend part of the application, the decision was made to use FastAPI as the main framework. It is a modern and high performance web framework used in building APIs with Python (**fastapi**). Based on the student's research, FastAPI seemed to be a good choice due to its ease of use, simplicity and good documentation available. The student also had previous experience with Python, making a Python-based framework an easy choice for this project. Finally, the reason for choosing a different, Python-based framework for the backend allows for more flexibility in the future, as the backend can be developed independently from the frontend and be re-used for different platforms, such as mobile or desktop applications.

The diagram 4.13 below shows how different components of the backend will interact with each other.

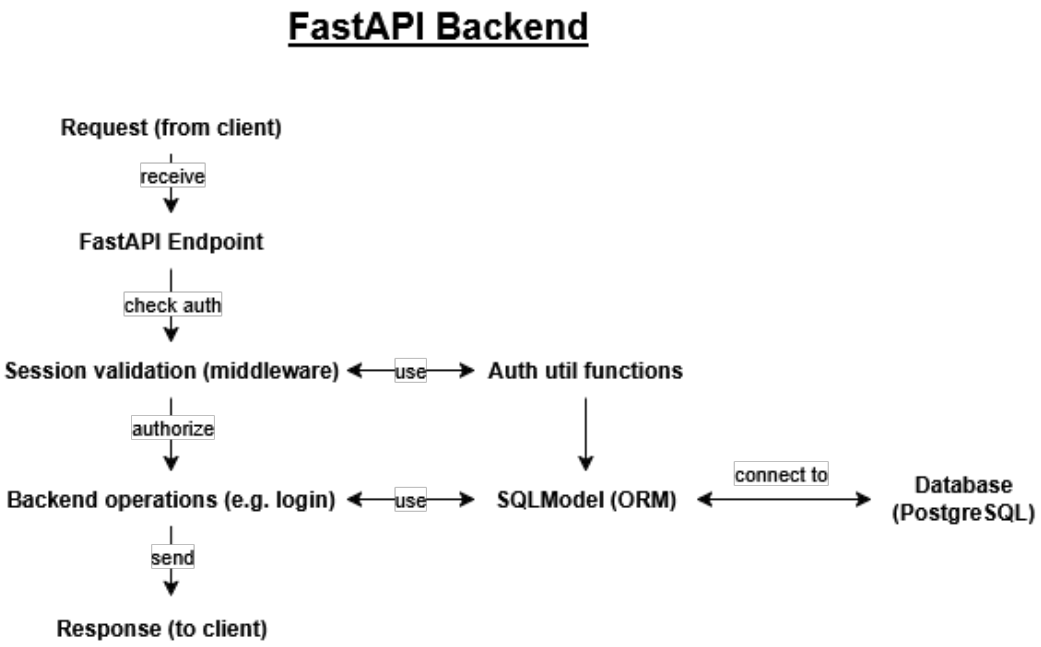


Figure 4.13: Interaction of Backend Components

4.4.3 Database

For the database, the student has chosen PostgreSQL, an open source relational database system that boasts a good reputation for its reliability, wide feature set and good performance and scalability (**postgres**). PostgreSQL supports a wide range of data types, including JSON and UUID, which are important for this project. Similarly, PostgreSQL offers robust security features like an access-control system, column or row-level security and secure connections with SSL, among others.

SQLModel, a Python library built on top of SQLAlchemy and Pydantic, will be used to interact with the database. SQLModel provides a way to define database tables using classes, which are then used to interact with the database, making it easier and safer to work with databases in the backend (**sqlmodel**).

4.5 Project Management

4.5.1 Methodology and Tools

Based on the research in section 3.1, the student has decided that he will be using a hybrid approach, with Waterfall as the main methodology for planning and managing the initial

part of the project, such as requirements gathering and the design of the system. The development part of the project will be done using ScrumBan, so that the student will be able to utilise elements from both frameworks. There are several reasons for this choice:

1. The nature of the project - the student is working on a project that has a limited timeframe (about 6-7 months) and is of a smaller scale.
2. Documentation requirements - the student is required to document the progress during the project in this report, including the requirements gathered, design considerations and implementation decisions and outcomes.
3. Regulatory requirements - the student is required to adhere to the regulations and standards of the healthcare industry, which may require extensive documentation and planning.
4. Customer involvement - the student will be working closely with the project stakeholder, who will be providing feedback and guidance throughout the project.
5. Familiarity with both Agile and Waterfall - the student has experience with both Agile (specifically Scrum and Kanban) and Waterfall methodologies, and has worked on projects that have used both approaches.

The student will use Notion as their project management tool, which is a comprehensive workspace that allows for task management, documentation, collaboration and knowledge sharing. Notion provides a wide range of features, including templates for Agile project management, creation of Agile elements like user stories, epics, backlogs, sprints and boards, and maitaining of documentation if necessary (**notion**).

4.5.2 Sprint planning

Based on the time remaining after the completion of the literature review, requirements gathering and system design, it was decided that only 6 sprints will be able to be completed before the project deadline. The sprints will be planned as follows:

- **Sprint 1** - Will focus on choosing the tech stack, installing the necessary tools and frameworks and setting up initial project files. Additionally, a basic frontend and backend will be created, with a focus on the basic functionalities like user authentication and registration and connection with the API/database.
- **Sprint 2** - Will focus on the patient profile, managing vaccines, allergies, medications and health data. The dashboard will also be created, with a basic layout and design.

- **Sprint 3** - Will focus on finishing the main dashboard and the upload and viewing of medical records and medical history.
- **Sprint 4** - Will focus on processing lab records with the LLM API and displaying them in tabular or graphical format.
- **Sprint 5** - Will focus on sharing records with doctors through various methods like email, share links or QR codes.
- **Sprint 6** - Will address any additional features or functionalities that need to be added, as well as any bugs or issues that need to be fixed.

Chapter 5

Development

This chapter will discuss the development of the project. Rather than going into detail how each sprint has been done, it will focus on the main features implemented, how this was achieved and will talk about successes or challenged that were encountered in the development process.

5.1 Sprint #1

The first sprint of this project was focused in laying the groundwork for the project, which mainly involved setting up the schemas for the ORM that would create the tables for the database, the initial setup of the API endpoints, such as the login and register endpoints, authentication and other security measures, but also setting up the frontend of the project.

5.1.1 SQLModel Schemas & Database creation

SQLModel played a pivotal role in helping quickly build the database tables. As previously mentioned in 4.4, SQLModel is built on top of SQLAlchemy and Pydantic, both being very powerful Python libraries. Pydantic was used to create the schemas that were used both within the backend but also by SQLAlchemy to create the tables in the database.

Below is an example of a schema that was used to create the User table in the database.

```
1 # Base model that contains the field serializer for date formatting to
      dd-mm-yyyy and the date field itself
2     class DateFormattingModel(SQLModel):
3         dob: date | None = None
```

```
4
5           @field_serializer('dob')
6           def serialize_dob(self, value: date) -> str:
7               return value.strftime("%d-%m-%Y")
8
9       class User(DateFormattingModel, table=True):
10          id: uuid.UUID = Field(default_factory=uuid.uuid4, primary_key=
    True)
11          name: str
12          email: EmailStr = Field(index=True, unique=True)
13          hashed_password: str
```

Listing 5.1: SQLModel User Schema

Similarly, SQLModel (and more specifically Pydantic schemas) could be used to create response/request models that would be used by the endpoints to validate the data that was being sent to or by the API. These schemas did not create tables in the database, but were used to control or validate the data being sent to or from the API.

Below is an example of a SQLModel/Pydantic schema that was used to validate the data that was being sent to the register endpoint.

```
1       # User Data model used for login and registration
2       class UserAuth(SQLModel):
3           email: EmailStr
4           password: str
5           name: str | None = None # Will only be used for registration
6
7       # User Data model used for most API responses
8       class UserPublic(SQLModel):
9           id: uuid.UUID
```

Listing 5.2: SQLModel Auth Schema

5.1.2 Authentication & APIs

As the project was centered around building a PHR system that would deal with sensitive health data, one of the main concerns was the security of the system and its users.

One of the important choices to make was how to handle the authentication. The student has identified 4 different ways to handle authentication in the project:

- JWT Tokens

- OAuth2
- Session-based authentication
- Using 3rd party authentication services, like Auth0

In the end, the student decided to go with a session-based authentication system. One of the main reasons was its ease of implementation that still provided a good level of security. The ability to control the session on the server side was an additional, important factor that contributed to this decision. This allows the system to safely log out users, invalidate sessions due to inactivity or suspicious activity, and also to control the session's lifetime, all without relying on storing tokens on the client side.

Sessions were created in the backend by storing them in a Session table in the database. The table contained a Session ID, which was passed to the user as a cookie. Upon a succesful login, the backend would set the cookie in the user's browser, which would then be sent with every request to the server.

To ensure that the cookies were safe from common attacks like Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF), the student used guidance from **owasp**; **mozilla** to set the following flags on the cookies:

```
    # Set the session cookie in the response and send it to the client
    response.set_cookie(
        "session_id",
        str(session_id), # Using str() to convert the UUID to a string
        httponly=True,
        max_age=3600, # 1 hour
        samesite="strict",
        secure=True
    )
```

To further secure the system, some of the endpoints that were created in this sprint were protected by using session validation checks to ensure that the user was authenticated before accessing the endpoint. This was achieved thanks to FastAPI's dependency injection system, which allowed the student to create a dependency that would check if the user was authenticated before allowing the request to continue. An example of this can be seen below:

```
    # Logout endpoint that uses the validate_session dependency to
    check if the user is authenticated
    @app.post("/logout")
    async def logout(response: Response, request: Request, user_id:
    uuid.UUID = Depends(validate_session), session: Session = Depends(
```

```
    get_session)):

        session_id = request.cookies.get("session_id")
        cookie_user_id = session.get(AuthSession, uuid.UUID(session_id
    )).user_id

        if cookie_user_id != user_id:
            raise HTTPException(status_code=403, detail="You do not
    have permission to log out this user")

        # Will use the end_session function to end the session in the
    database
        end_session(request, session) # Need to pass the request and
    session to the function, otherwise it will not work

        # Still need to delete the session cookie from the client
        response.delete_cookie(
            "session_id",
            samesite="strict",
            secure=True,
            httponly=True
            )

        return {
            "status": status.HTTP_200_OK,
            "message": "Logout successful"
        }

    # Util function to validate the session and return the user_id -
    also used as a dependency for protected routes
    async def validate_session(request: Request, session: Session =
    Depends(get_session)):
        session_id = request.cookies.get("session_id")
        if not session_id:
            raise HTTPException(status_code=status.
    HTTP_401_UNAUTHORIZED, detail="Session cookie not found")

        existingAuthSession = session.exec(select(AuthSession)
                                .where(AuthSession.id == uuid.UUID(
    session_id))
```

```
                                    .where(AuthSession.expires_at >
    datetime.now())
        ).first()

        if not existingAuthSession:
            raise HTTPException(status_code=status.
    HTTP_401_UNAUTHORIZED, detail="Session not found")

        return existingAuthSession.user_id
```

Listing 5.3: FastAPI Dependency for Session Validation

Finally, to ensure that the system was secure, the system also used a hashing algorithm to hash the passwords before storing them in the database. The student identified multiple hashing algorithms that could be used, with the main contenders being bcrypt, scrypt and Argon2.

In the end, the decision was made to use bcrypt as the hashing algorithm. The main reasons for the use of this algorithm was its simplicity of use, wide adoption and its balance between security and perfomance. The passlib library was used to hash the passwords before storing them in the database. The library allowed for automatic salt generation and storage within the hash and by default, it used a work factor of 12, which is considered to be a good balance between security and performance. An example of this can be seen below:

```
    # Util function to verify the password hash against the plaintext
    password
    def verify_hash(plaintext_password: str, hashed_password: str) ->
    bool:
        return bcrypt.verify(plaintext_password, hashed_password)

    # Util function to create a password hash from the plaintext
    password
    def create_hash(plaintext_password: str) -> str:
        return bcrypt.hash(plaintext_password)
```

Listing 5.4: Hashing passwords with bcrypt

A final security measure that could've been implemented was a rate limiter to all of the created endpoints. Similarly, Starlette, the framework FastAPI was built on top of, also offered other middleware such as HTTPSRedirectMiddleware, TrustedHostMiddleware, and others that could be used to further secure the system. However, in the interest of time, it was decided to leave these for a future sprint.

5.1.3 Frontend Setup

While most of the work done in this sprint was done in the backend, some work was also done in the frontend, mainly focusing on the login and register pages. Here, the student used the PrimeVue component library to quickly and easily create the forms that would be used to log in and register users.

An example of PrimeVue components being used can be seen below in the Register page. Some of the components taken from PrimeVue include InputText, DatePicker, Password, Button and Message.

```
    <Form
        v-slot="$form"
        :initialValues
        :resolver
        @submit="onFormSubmit"
        class="flex flex-col gap-4 w-full sm:w-60"
      >
        <div class="flex flex-col gap-1">
          <InputText name="name" type="text" placeholder="Nume" fluid
/>
          <Message
            v-if="$form.name?.invalid"
            severity="error"
            size="small"
            variant="simple"
            class="text-rose-600 text-sm"
            >{{ $form.name.error.message }}</Message
          >
        </div>
        <div class="flex flex-col gap-1">
          <InputText name="surname" type="text" placeholder="Prenume"
fluid />
          <Message
            v-if="$form.surname?.invalid"
            severity="error"
            size="small"
            variant="simple"
            class="text-rose-600 text-sm"
            >{{ $form.surname.error.message }}</Message
          >
```

```
      </div>
      <div class="flex flex-col gap-1">
        <DatePicker
          name="dob"
          dateFormat="dd/mm/yy"
          placeholder="Data nasterii"
          showIcon
          fluid
          :maxDate="maxDate"
        />
        <Message
          v-if="$form.dob?.invalid"
          severity="error"
          size="small"
          variant="simple"
          class="text-rose-600 text-sm"
          >{{ $form.dob.error.message }}</Message
        >
      </div>
      <div class="flex flex-col gap-1">
        <InputText name="email" type="text" placeholder="Adresa email" fluid />
        <Message
          v-if="$form.email?.invalid"
          severity="error"
          size="small"
          variant="simple"
          class="text-rose-600 text-sm"
          >{{ $form.email.error.message }}</Message
        >
      </div>
      <div class="flex flex-col gap-1">
        <Password name="password" placeholder="Parola" :feedback="false" toggleMask fluid />
        <Message
          v-if="$form.password?.invalid"
          severity="error"
          size="small"
          variant="simple"
          class="text-rose-600 text-sm"
```

```
67            >
68              <ul class="my-0 flex flex-col gap-1">
69                <li v-for="(error, index) of $form.password.errors" :key
    ="index">
70                  {{ error.message }}
71                </li>
72              </ul>
73            </Message>
74          </div>
75          <Button type="submit" severity="secondary" label="Inregistrare
    " />
76        </Form>
```

Listing 5.5: PrimeVue components in the Register page

As previously mentioned in 4.4, Vue also comes with other in-built tools that help create a well-working frontend. One of these tools is Vue Router, which was used to create the routes for the frontend. The student created a simple router that would allow the user to navigate between different pages. A navigation guard was used to protect the routes that required the user to be authenticated. An example of this can be seen below:

```
1     // Navigation guard
2 router.beforeEach(async (to) => {
3   const authStore = useAuthStore()
4
5   if (to.meta.requiresAuth) {
6     await authStore.checkAuth() // Check if user is authenticated for
      protected routes
7     if (!authStore.isAuthenticated) {
8       return { name: 'Login' } // Redirect to login if not
      authenticated
9     }
10  } else if (to.path === '/login' || to.path === '/register') {
11    await authStore.checkAuth()
12    if (authStore.isAuthenticated) {
13      return { name: 'Dashboard' } // Redirect to dashboard if
      authenticated and going to login or register
14    }
15  }
16
17  return true // Continue to requested route if no conditions are met
```

```
})

export default router
```

Listing 5.6: Vue Router Navigation Guard

Similarly, Pinia store was used to manage the authentication state of the user in the frontend. The store was then used by elements like the Navigation Guard to check if the user was authenticated before allowing them to access certain routes. An example of the store can be seen below:

```
export const useAuthStore = defineStore('auth', () => {
  const isAuthenticated = ref(false)
  const user = ref(null)

  async function checkAuth() { // Function checks if user is authenticated
    try {
      const response = await api.get('/me') // This will return the user object if the user is authenticated
      isAuthenticated.value = true // if you get response, then user is authenticated
      user.value = response.data.user
    }
    catch {
      isAuthenticated.value = false // if you don't get response, then user is not authenticated
      user.value = null
    }
  }
  return { isAuthenticated, user, checkAuth }
})
```

Listing 5.7: Pinia Store for Authentication

5.2 Sprint #2

The second sprint of this project was focused on building some of the smaller elements of the system, such as the ability to add vaccines, allergies and medications. The decision to start with the smaller elements was made to allow the student to get a better understanding

of how the frameworks used in the project worked and to get a better understanding of how to structure the project.

5.2.1 Adding Vaccines, Allergies and Medications functionality

The student started by creating the schemas for the Vaccines, Allergies and Medications tables in the database. These tables were created in a similar way to the User table, using SQLModel schemas. Afterwards, the student created the endpoints that would allow the user to add, update, delete and view the data in these tables. An example of the schema for the Vaccines table and the endpoint to add a vaccine can be seen below:

```
    # Vaccine Table model used for table creation
    class Vaccine(SQLModel, table=True):
        id: uuid.UUID = Field(default_factory=uuid.uuid4, primary_key=
    True)
        name: str
        provider: str
        date_received: date

        user_id : uuid.UUID = Field(foreign_key="user.id")
        user: User = Relationship(back_populates="vaccines")

        certificate: Optional["FileUpload"] = Relationship(
    back_populates="vaccine", cascade_delete=True)

        @field_serializer('date_received')
        def serialize_date_received(self, value: date) -> str:
            return value.strftime("%d-%m-%Y")


    # Add a vaccine endpoint
    @app.post("/me/vaccines")
    def add_vaccine(vaccine: VaccineCreate, user_id: uuid.UUID =
    Depends(validate_session), session: Session = Depends(get_session)
    ):
        user = session.get(User, user_id)

        # Create vaccine using Vaccine main schema
        new_vaccine = Vaccine(
            name = vaccine.name,
            provider = vaccine.provider,
```

```
            date_received = vaccine.date_received,
            user = user)

        session.add(new_vaccine)
        session.commit()
        session.refresh(new_vaccine)

        # Create a response object to return to the user using the VaccineResponse schema
        vaccine_response = VaccineResponse(
            id = new_vaccine.id,
            name = new_vaccine.name,
            provider = new_vaccine.provider,
            date_received = new_vaccine.date_received
        )

        return {
            "status": status.HTTP_201_CREATED,
            "message": "Vaccine added successfully",
            "vaccine": vaccine_response
        }
```

Listing 5.8: SQLModel Vaccine Schema

On the frontend side, the system used Vue's main strengths to enable a smooth developer and future user experience. Some of the strengths used were using Vue components to create reusable elemenets, such as a Vaccine Card that would be used to display the vaccines that the user had added. The card also used other Vue elements such as props and emits to pass data between parent and child elements and pass events, respectively. An example of the Vaccine Card can be seen below:

```
    <template>
  <Card style="overflow: hidden" class="w-full" :pt="cardStyles">
    <template #title>
      <span class="font-bold text-2xl">{{ name }}</span> <!-- Name of the vaccine passed as a prop by the parent element -->
    </template>
    <template #subtitle>
      <div class="flex items-center justify-between">
        <div class="flex flex-col justify-start">
          <span class="font-bold">{{ provider }}</span>
```

```
          <span>{{ date_received }}</span>
        </div>
        <div>
          <Button
            icon="pi pi-eye"
            class="p-button-rounded p-button-text p-button-plain"
            @click="emit('showFile', props.id)" <!-- Emit an event to show the certificate -->
            v-if = "hasCertificate"
          />
          <Button
            icon="pi pi-ellipsis-h"
            class="p-button-rounded p-button-text p-button-plain"
            @click="toggle"
            aria-haspopup="true"
            aria-controls="overlay_menu"
          />
          <Menu ref="menu" id="overlay_menu" :model="items" :popup="true" />
        </div>
      </div>
    </template>
  </Card>
</template>
```

Listing 5.9: Vue Vaccine Card

Subsequently, using this VaccineCard element is very easy in the main vaccine view page:

```
    <div class="flex flex-col items-center gap-4 p-3 md:p-5">
      <ProgressSpinner v-if="loading" />

      <div v-else-if="error" class="p-4 text-red-500">
        {{ error }}
      </div>

      <div v-else-if="vaccines.length === 0" class="p-4">Nu a fost gasit nici un vaccin.</div>

      <VaccineCard
        v-else
        v-for="vaccine in vaccines"
```

```
        :key="vaccine.id"
        v-bind="vaccine"
        :has-certificate="vaccine.certificate ? true : false"
        @delete="deleteVaccine"
        @open-edit="openEditDialog"
        @show-file="showCertificate"
      />
    </div>
```

Listing 5.10: Vue Vaccine View Page

This format was used across the system to easily create reusable components that could be used in multiple places, making the system more modular and easier to maintain.

To make sure the data displayed in the frontend was always up to date, the frontend used Vue's reactivity system. This allowed the data to be automatically updated whenever any change was made to the data in the backend or frontend. Examples of the reactivity system in use can be seen below, with functions that add and delete vaccines from the frontend when called:

```
    <script setup>
    import { onMounted, ref } from 'vue'

    const vaccines = ref([])
    onMounted(async () => {
  try {
    const response = await api.get('me/vaccines')
    vaccines.value = response.data
  } catch (err) {
    error.value = 'A aparut o eroare la incarcarea vaccinelor' + err
  } finally {
    loading.value = false
  }

  const addVaccine = (vaccine) => {
  vaccines.value.push(vaccine)
}

const deleteVaccine = (id) => {
  vaccines.value = vaccines.value.filter((vaccine) => vaccine.id !==
    id)
}
```

```
})
```

Listing 5.11: Vue Reactivity System

5.2.2 File Uploads

Another major feature that was implemented in the 2nd sprint was the ability to upload files. At the time of implementation, the feature was only to be used for uploading vaccine certificates, however it could be easily extended to other parts of the system, such as uploading health records or lab results.

To allow a proper upload of files, a new table was created in the database, called FileUpload. This table contained the file metadata, such as its name, size, type, path and others.

To add more security to the system, the files were further encrypted before being stored in the database. The encryption was done using the Fernet symmetric encryption algorithm from the cryptography library. Fernet uses AES-128 to encrypt the files. The key used to encrypt the files was stored in the environment variables and was generated when the system was started. In the interest of time, no rotation system for the key was implemented, however this would be a good feature to add in the future.

The file upload process can be seen in the diagram below:

The file upload process was done in two steps. The first step was to upload the file to the server by using multipart form data. The next step would have the file be validated by checking its file type and size, then encrypted and stored in the file system and database.

To access the files, the system used a new endpoint that would allow the user to download the file. The endpoint would take the file ID as a parameter and would stream the file to the user. The endpoint can be seen below:

```
    # Get a file by ID
@app.get("/files/{record_type}/{record_id}")
async def get_file(
    record_type: str,
    record_id: uuid.UUID,
    user_id: User = Depends(validate_session),
    session: Session = Depends(get_session)
):

    print(f"GET request received for vaccine file: {record_id}")

```

```
    record = await get_connected_record(record_type, record_id, user_id, session)

    file_record = None

    if record_type == "vaccine":
        file_record = record.certificate


    if not file_record:
        raise HTTPException(status_code=status.HTTP_404_NOT_FOUND, detail="File not found")

    async def get_data_from_file():
        with open(file_record.file_path, "rb") as f:
            encrypted_content = f.read()

        decrypted_content = decrypt_file(encrypted_content)

        yield decrypted_content

    return StreamingResponse(
        content=get_data_from_file(),
        media_type=file_record.file_type,
        status_code=status.HTTP_200_OK,
        headers={"Content-Disposition": f"inline; filename={file_record.name}"}
    )
```

Listing 5.12: File Download Endpoint

5.3 Sprint #3

5.4 Sprint #4

5.5 Sprint #5

5.6 Sprint #6

Chapter 6

Evaluation

6.1 Deployment

6.2 System Testing

6.3 User Acceptance Testing

6.4 Client feedback

Chapter 7

Conclusion and Future Work

7.1 Areas of Improvement

7.2 Future Work

7.3 Lessons Learned and Reflections

7.4 Final Thoughts

Appendix A

Requirements

ID	Requirement	Priority
1.1	The system must be accessible on all modern desktop and mobile-based browsers.	Must Have
1.2	The system must be accessible from any location by using an internet connection.	Must Have
1.3	The system must store the data in a secure manner, ensuring that only the patient and the doctor can access the data.	Must Have
1.4	When shared with the doctor via a link, the system must load within 3 to 5 seconds when accessed via a desktop browser.	Should Have
1.5	When shared with the doctor via a link, the system should secure the data with a unique token or PIN that expires after the specified time frame.	Could Have
1.6	The system could be accessible on all modern mobile devices via a mobile application.	Could Have

Table A.1: Non-functional Requirements

ID	Requirement	Priority
2.1	The system must provide a secure login mechanism for patients via Multi Factor Authentication.	Must Have
2.2	If used on mobile, the system should allow the patient to use biometric authentication for logging in.	Should Have

Table A.2: Login Requirements

ID	Requirement	Priority
3.1	The system must allow patients to upload their own medical records in a variety of formats (PDF, DOC, etc).	Must Have
3.2	The system must allow the patient to specify and categorise the type of document they are uploading (lab test, doctor consultation, etc).	Must Have
3.3	If used on mobile, the system should allow the patient to take a picture of the document and upload it.	Could Have

Table A.3: Document Upload Requirements

ID	Requirement	Priority
4.1	The system must allow the patient to generate a shareable link to provide access to their medical records.	Must Have
4.2	When creating the shareable link, the system must allow the patient to set an expiration date for the link.	Must Have
4.3	When creating the shareable link, the system should allow the patient to set an access password for the link.	Should Have
4.4	When creating the shareable link, the system should allow the patient to select which records to share with the doctor.	Should Have

Table A.4: Patient Shareable Link Requirements

ID	Requirement	Priority
5.1	The patient personal cabinet must provide an overview of the patient's history through 3 main sections: personal information, lab tests, and doctor consultations.	Must Have
5.2	The system must display the patient's history in a chronological order in the form of a timeline.	Must Have
5.3	The system must allow patients to add their own personal information, such as name, date of birth, or address.	Must Have
5.4	The system must allow the patient to add their own allergies.	Must Have
5.5	The system must allow the patient to add their own vaccinations.	Must Have
5.6	When viewing doctor consultations, the system should divide them into categories based on the domain of the doctor (cardiology, neurology, etc).	Should Have
5.7	The system should allow the patient to enter vitals information, such as height, weight, blood pressure, etc.	Should Have
5.8	When multiple vital entries are made, the system could display a historical graph of the patient's vitals.	Could Have
5.9	The system could allow the patient to switch between viewing the lab tests in the document format or in a tabular, numerical format.	Could Have

Table A.5: Patient Personal Cabinet Requirements

ID	Requirement	Priority
6.1	The system must provide an overview of the patient history through 3 main sections: personal information, lab tests, and doctor consultations.	Must Have
6.2	When shared with the doctor, the system must allow the doctor to only view the patient's history, not edit it.	Must Have
6.3	The system must allow the doctor to view blood tests in a graphical format.	Must Have
6.4	The system must allow the doctor to view blood tests in a numerical, tabular format.	Must Have
6.5	The system must allow the doctor to view the patient's history in a chronological order.	Must Have
6.6	The system must display the doctor consultation and every lab test, except for blood tests, in a free text or document format.	Must Have
6.7	When viewing blood test results, the system should show the source document of the blood test value.	Should Have
6.8	For blood test results, the system should display the normal range values for each test.	Should Have

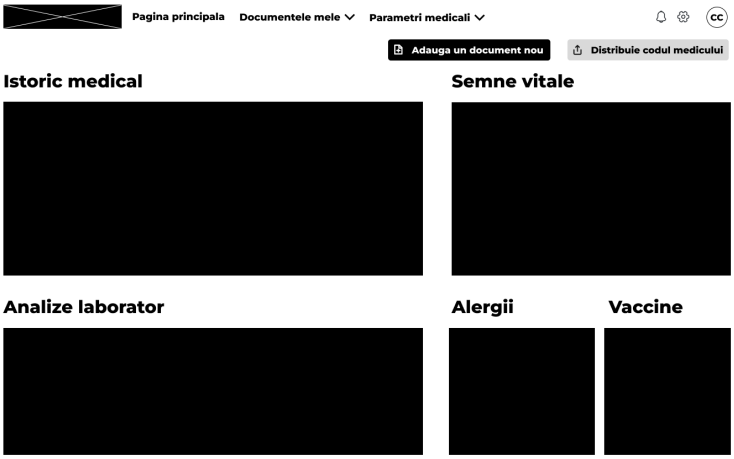
Table A.6: Shared Patient Information Requirements (Doctor View)

ID	Requirement	Priority
7.1	The system must allow patients to enter their current medication including details such as the name of the drug, dosage, frequency and start/end date.	Must Have
7.2	The system must allow patients to add new medication to their list.	Must Have
7.3	When adding medication, the system should have 2 options: add a simplified version of the medication or add a detailed version of the medication.	Should Have
7.4	When choosing the simplified version, the system should allow the patient to just add the name, dosage and duration of the medication.	Should Have
7.5	When choosing the detailed version, the system should allow the patient to add the name, dosage, frequency, start/end date, and the reason for taking the medication.	Should Have
7.6	The system should allow patients to add their past medication	Should Have
7.7	The system should allow patients to set medication reminders.	Should Have
7.8	After entering the medication, the system could allow the patient to track the medication intake.	Could Have

Table A.7: Patient Medication Requirements

Appendix B

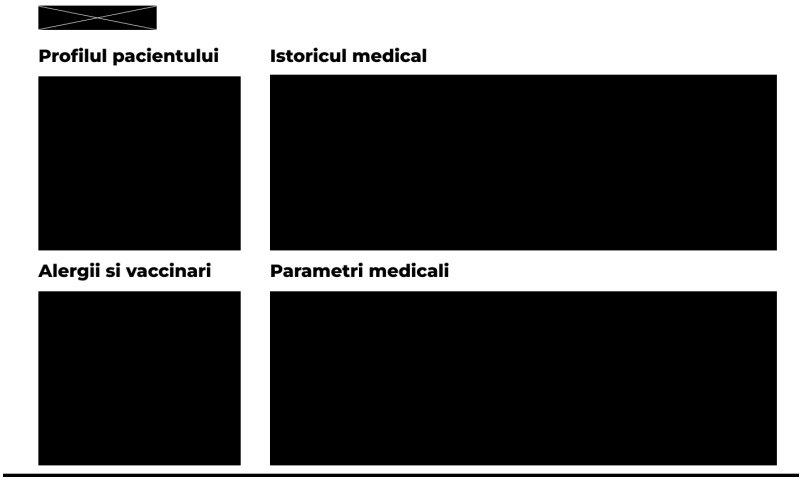
Wireframes



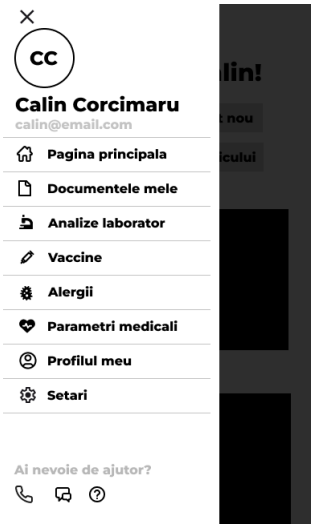
(a) Desktop version

(b) Mobile version

Figure B.1: Desktop and Mobile version of the Dashboard screen

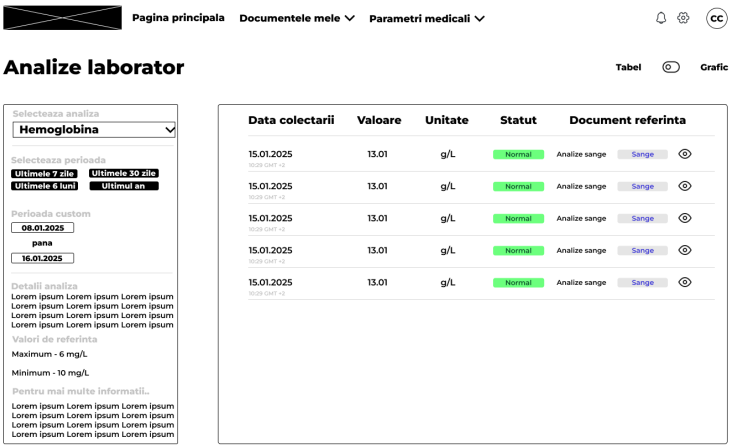


(a) Desktop version



(b) Mobile version

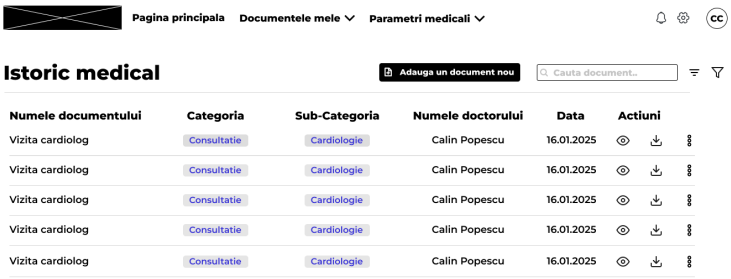
Figure B.2: Desktop and Mobile version of the Doctor View screen



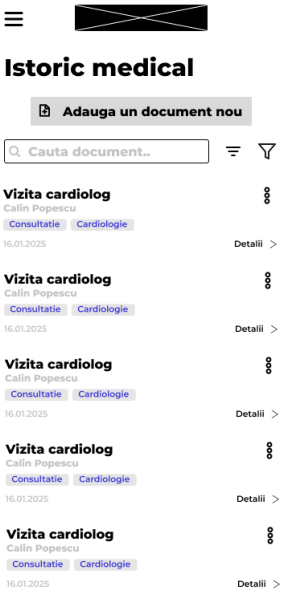
(a) Desktop version

(b) Mobile version

Figure B.3: Desktop and Mobile version of the Lab Test screen

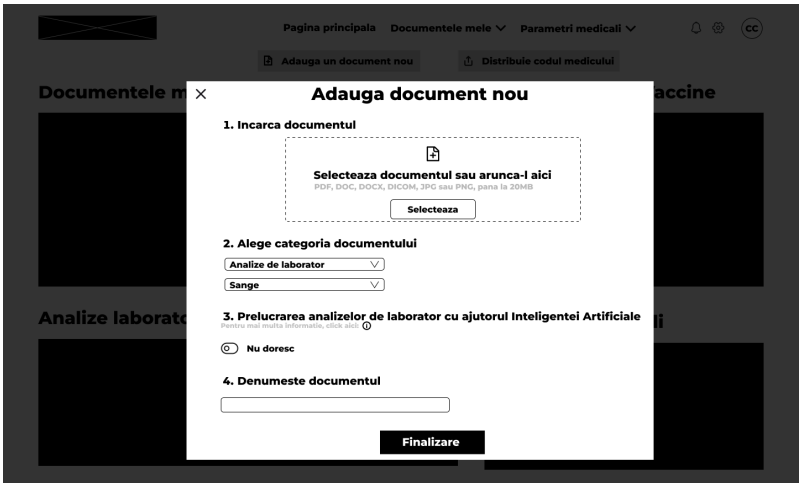


(a) Desktop version

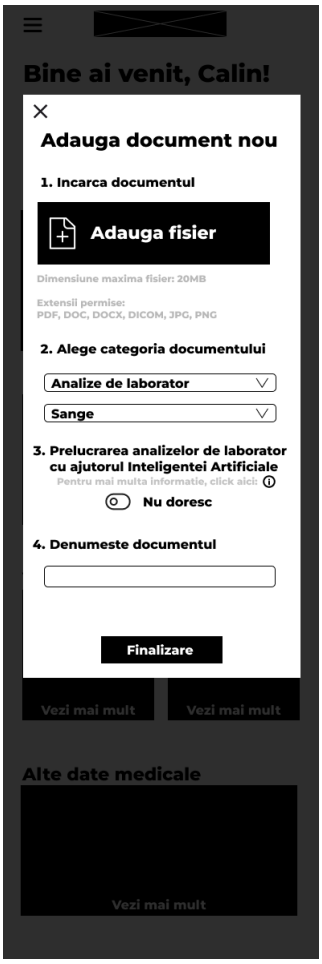


(b) Mobile version

Figure B.4: Desktop and Mobile version of the Medical History screen

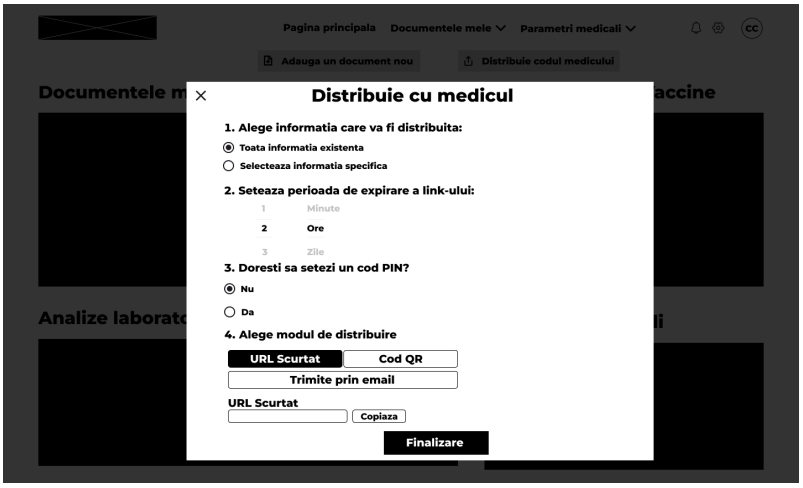


(a) Desktop version

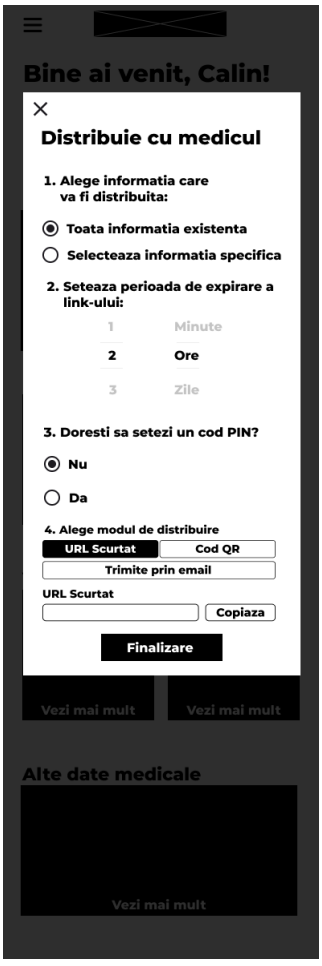


(b) Mobile version

Figure B.5: Desktop and Mobile version of the New Document screen

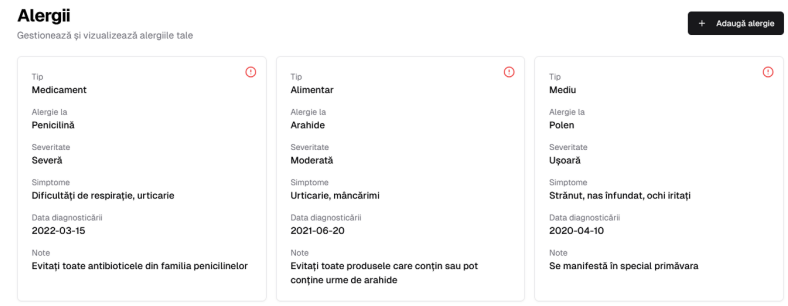


(a) Desktop version



(b) Mobile version

Figure B.6: Desktop and Mobile version of the Share Doctor screen



(a) Desktop version

(b) Mobile version

Figure B.7: Desktop and Mobile version of the Allergies screen

Figure B.8: Mobile version of the Vaccines screen