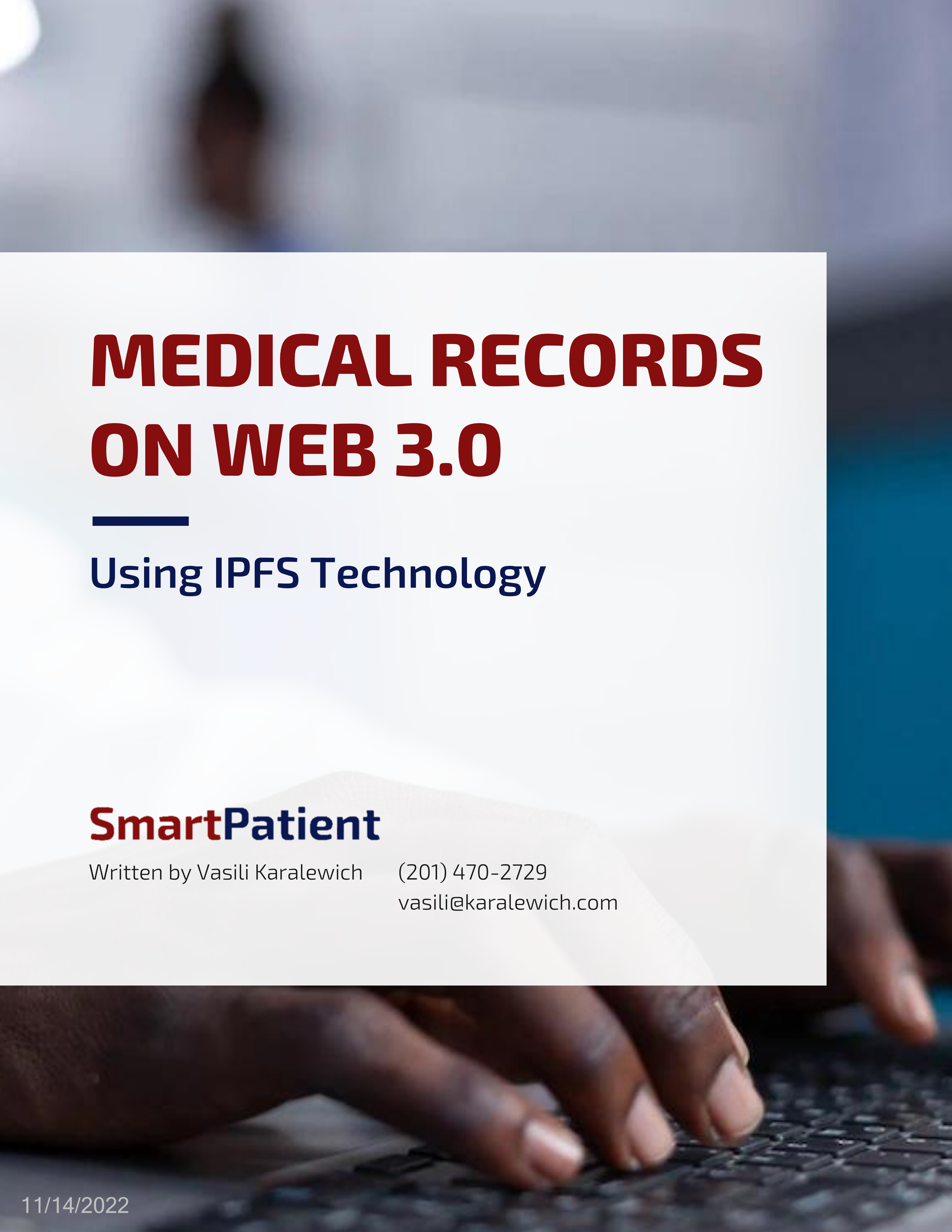


MEDICAL RECORDS ON WEB 3.0

Using IPFS Technology

SmartPatient

Written by Vasili Karalewich

(201) 470-2729
vasili@karalewich.com

11/14/2022

Medical Records on Web 3.0

Introduction

SmartPatient allows people to control their medical records on a decentralized network, rather than letting all their doctors store some version of it. This technology ensures that records are never lost, and it allows patients to be the only ones who control the access of their data. Patients only need to fill their medical records once, and changes made by doctors update for all doctors that the patient uses. Insurance companies also have the ability to be added, and patients are only allowed to edit certain information.

THE INTERPLANETARY FILE SYSTEM (IPFS)

A single universal medical record is no new concept. There are many other companies that attempt to accomplish this task. However, these companies use a centrally located server to store their patients' medical information (…yikes). This already reduces the security of their patients' information, no matter how they try to increase it. As opposed to a centrally located server, IPFS is built around a decentralized system of user-operators who hold portions of the overall data, creating a resilient system of file storage and sharing.

HOW IPFS WORKS

IPFS addresses a file by *what's in it*, or by its *content*. Right now, the internet does not do this[1]. It addresses files by its location, using URLs such as these:

> https://en.wikipedia.org/wiki/Doctor_(title)
> C:\Users\Joe\My Documents\presentation.ppt

The content is identified by a *cryptographic hash*. The hash is unique to its content, even though it may look short compared to the original content. Hashes turn content into a combination of numbers and letters.

[1]: It is like when you go to a library–you look for content (book title, genre, etc.). You would never go to a library and say you want the book on the second floor, first stack, third shelf from the bottom, and four books from the left. If someone moves the book, you're out of luck!

For example, one type of hash is SHA-256. It turns the word hello into:
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

SHA-256 is part of the SHA-2 family of one-way cryptographic functions, developed in 2001 by the United States National Security Agency (NSA). Decrypting keys with “brute-force” is not possible. SHA-256 is not the only cryptographic function that IPFS uses. With Multibase technology, IPFS can use many different types of encryptions to increase security and compatibility. All cryptographic functions have the following four properties:

1. **Deterministic** – the same input message always returns the same output hash.
2. **Uncorrelated** – a small change in the message should generate a completely different hash
3. **Unique –** it’s infeasible to generate the same hash from two different messages
4. **One-way** – it’s infeasible to guess or calculate the input message from its hash.

More information on encryption and cryptography will be discussed later.

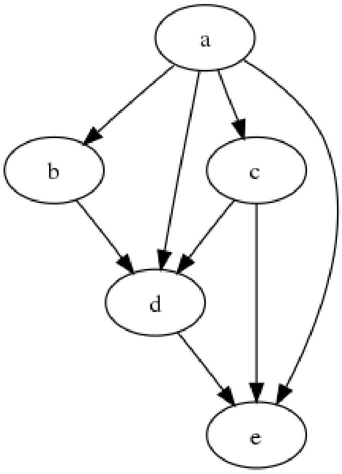


Figure 1: A five node acyclic diagraph.

IPFS access files using a mathematical graph theory called **Acyclic Diagraphs**. It consists of vertices and edges (arcs), with each edge directed from one vertex to another, such that following those directions will never form a closed loop. This concept is commonly described in biology (evolution, family trees, and epidemiology).

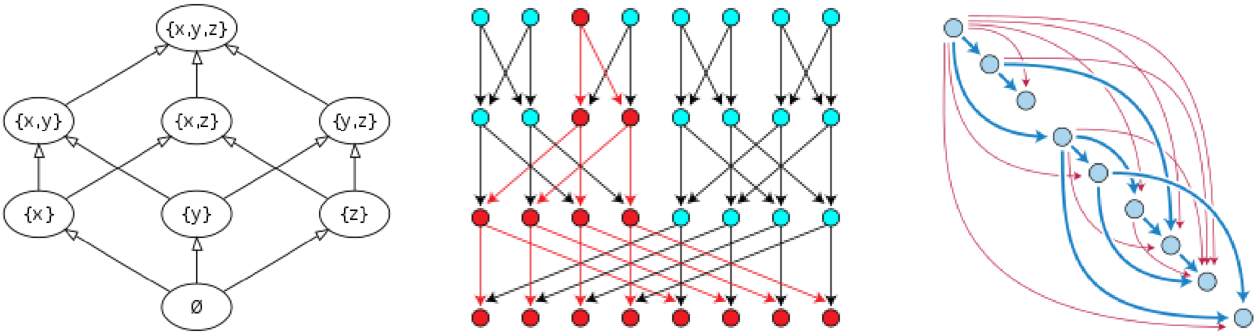


Figure 2A, 2B, 2C: More complex acyclic diagraph examples.

Versions of this technology that are much more complex, allow IPFS to break your data into small pieces and store them away in different spots across the internet. Since this data is one-way, it can only be accessed from a single identifier key (CID), which only the user will have access to.

There are two types of encryptions: transport-encryption and content-encryption. Since IPFS only covers transport-encryption, SmartPatient encrypts all data uploaded to IPFS to add an additional layer of security and privacy for patients.

Additional complexity is introduced to the technology when making changes to a file. Since IPFS generates hashes based on file content, changing a files content will also change the hash. Therefore, mutable pointers are used so that new versions can be kept under the same key. This technology is called IPNS. DNSLink is also an alternative as well and is much faster than IPNS.

SMARTPATIENT'S PLAN

Patients should have access to their records, on their phones, at all times. With major privacy concerns though, we do not consider storing this data on a central database as a valid solution. The technology of Web 3.0 and IPFS offers the privacy and security that a central database will never provide.

With one singular medical record, patients will never have to spend time writing out their medical history again. In fact, SmartPatient will change the way that people get medical care. Since they have a singular medical record that is live and easily transferable, they can go to any doctor they want.

In our app, we will make it possible for patients to find doctors based on their preferences, whether that be: experience, distance, or current availability of appointments. Patients will be able to schedule appointments on their terms and won't have to worry about having to transfer data between doctors.

While medical visits become more likely with age, a whopping 40% of young adults between the ages of 18 to 24 did not visit a provider at all during the year, according to a sampling from the U.S. 2010 Census. An app that encourages people to be health conscious and makes it easy to pick any doctor is appealing to younger adults who do not feel that a well visit is worth all the scheduling and planning trouble.

TAP TO TRANSFER MEDICAL RECORDS USING NFC

Imagine this: Instead of spending 20 minutes filling out online forms before you go to an urgent care, you just walk in, open up the SmartPatient app, and tap your phone at the doctor's office, and your whole medical profile gets transferred to them.

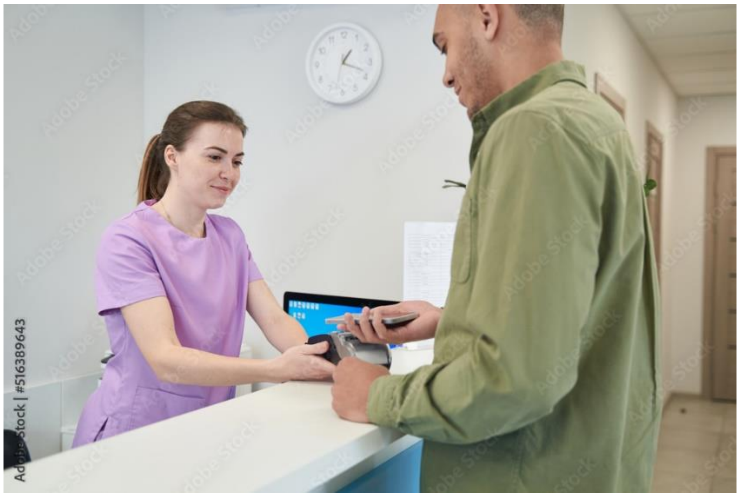
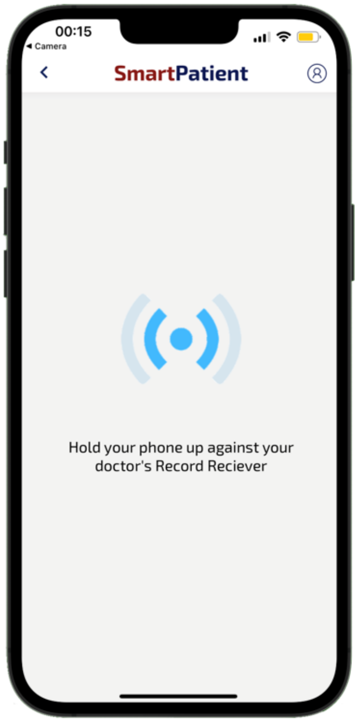


Figure 3: Patient gives his medical records to this doctor by tapping his phone on their NFC reader, which eliminates the need for filling out forms and questionnaires about medical history.

Now they have a key to your medical profile, and they can make edits and updates as necessary. Then, before you leave, you tap your phone again and your medical record gets updated.

The technology that makes this possible is called Near Field Communication (NFC). It enables communication between two electronic devices over a distance of 4 cm or less. Using inductive coupling between two nearby loop antennas, an air-core transformer is effectively formed. What this means, is that radio waves are generated which can be used to transfer information. NFC technology is open-source and runs on unlicensed radio frequencies; however, there are many standards such as ISO/IEC, GSMA, and StoLPaN, some of which are followed by Apple and Android. This technology is commonly used for Apple Pay, in which card information is encrypted and scanned by an NFC reader.

Tapping to Transfer your medical record, which we will call TapPatient, will really hit home the point that the medical records only belong to the patient, and that they are in control of them. Just like Apple Pay, when you open the TapPatient screen, Face ID or a passcode will be required for increased security.



Hold your phone up against your doctor's Record Reciever

Figure 4: TapPatient Screen on the app, coded in React Native which is used for many apps on the Apple and Google Play App Stores.

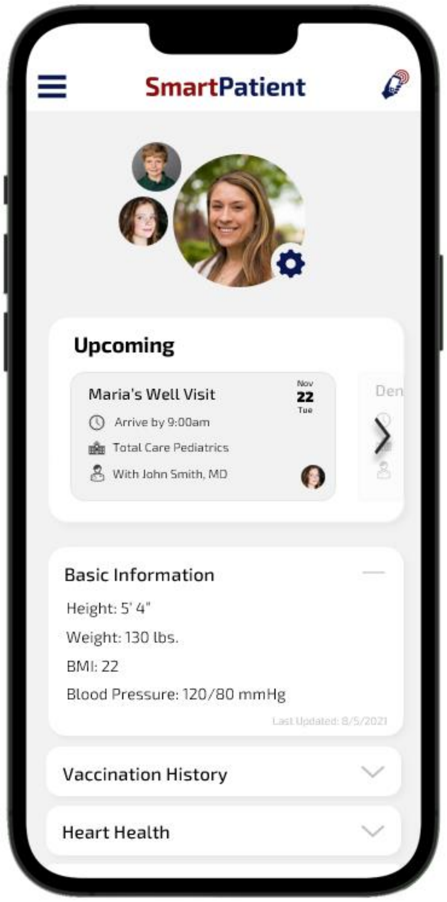
Additional options will be available to only share certain information, such as basic health information, or a single immunization, instead of giving all your records away at each tap.

THE SMART PATIENT APP

The Smart Patient App has the opportunity to house many different features: the medical profile, appointment scheduler, telemedicine, and TapPatient as discussed in the prior section.

The medical profile will give people access to their own medical records at any time. Whether this be for motivation to stay healthy, or to learn more about themselves, there is no reason that people should be left to wonder what types of vaccinations they do or do not have, because it is stowed away at their doctor's office.

It will be intuitive and simple, despite storing a lot of important information. The first prototype of the medical profile was coded on an iPhone, but we still need more feedback from doctors and patients regarding the placement and inclusion of certain information.



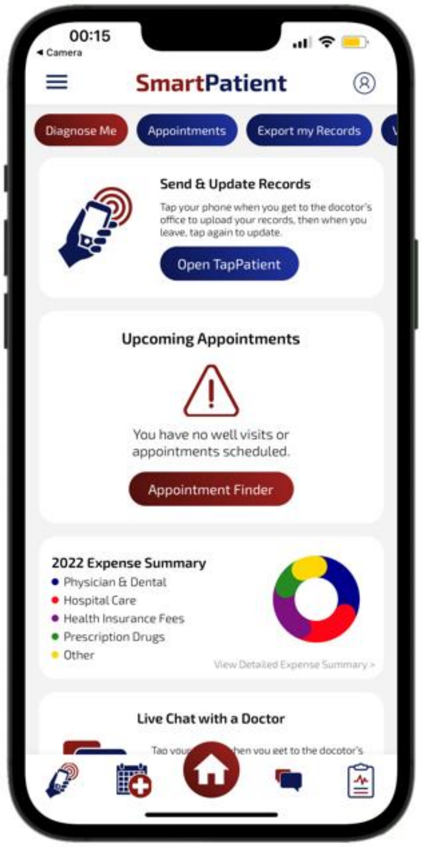
Maria's Well Visit
Nov 22 Tue
Arrive by 9:00am
Total Care Pediatrics
With John Smith, MD

Basic Information
Height: 5' 4"
Weight: 130 lbs.
BMI: 22
Blood Pressure: 120/80 mmHg
Last Updated: 8/5/2021

Figure 5: Tap Patient Medical Profile

This graphic displays our prototype of the medical profile. As shown, parent's have the option to view their child's medical records in the app as well. This screen also displays upcoming appointments, and then below that is the health information.

We would like to get more feedback on the best way to display this information, from patients and doctors. Right now, we have grouped them into dropdowns, which reveal information when clicked.



Tap your phone when you get to the docotor's office to upload your records, then when you leave, tap again to update.

You have no well visits or appointments scheduled.

Figure 6: Home page widgets of the app

Additional ideas we would like to incorporate into the app include the Appointment Finder, which makes it easier to find doctors so you can pick an appointment at your convenience, and make sure that you are going to the right doctors. The app can even recommend going to certain specialized doctors every so often.

Expense summaries are also included in the home screen. We are not sure if this data will be fed directly from doctors and insurance companies, or if it is user inputted, but the idea is for people to keep track of and budget their medical expenses easily.

The home screen will also display your prescriptions and what you should be taking and when just in case you forget. Ideally this information will be inputted by the doctor into the medical record and automatically be displayed by the app.

We also have a widget for live chat with a doctor, which could include telemedicine if we decide to go down that route, although starting off with that feature may be difficult because we would need doctors to participate from the start, so it probably isn't practical.

CONCLUSION

This document describes some of our initial ideas and plans for this company. We hope that this technology could be used to transform the way healthcare is delivered. We hope to get feedback on these ideas in the coming weeks and revisit this document.