MetroStar Systems®

Provider User-Experience Challenge

Locket for Providers

March 23, 2016

Prepared For:
The Department of Health and Human Services Provider User-Experience Challenge

Prepared By:
Neysa Spence
Contracts Manager

MetroStar Systems, Inc.
1856 Old Reston Avenue, Suite 100
Reston, VA 20190-3330

Telephone: 703-481-9581
nspence@metrostarsystems.com
contracts@metrostarsystems.com

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of—or in connection with—the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. All data contained herein is subject to this restriction.

Table of Contents

1.0. Intro

MetroStar Systems, an award winning technology company in Northern Virginia, has developed many web and mobile applications for both private companies and government agencies. Recent highlights include winning third place in the NIST Reference Data Challenge, developing a prototype of a game that teaches displaced Syrian refugee children to read, and developing health IT solutions for several clients. Riding the wave of these recent successes, we are encouraged to apply for this challenge and to continue providing value to the healthcare domain.

MetroStar is well situated to address the concerns of the health consumer challenge by 1) providing a platform to transfer patient data from Electronic Health Records (EHRs) to patient mobile devices and 2) reducing the amount of redundant paperwork that consumers have to fill out at every location. The consumer app will have a way for patients to view and manage all of their own health data in one location. Furthermore, it will streamline both checking into appointments (via a QR code scanner) and managing multiple family members' medical information. When the consumer checks into a new health clinic, he or she may allow the clinic to access and upload all of his or her existing data. In addition to streamlining the transfer of information and providing a repository for a family's health information, the application provides a suite of tools that helps to make medical compliance easier through a medication subscription manager and reminders to follow recommendations from healthcare providers.

This proposed platform is called ***Locket***. ***Locket*** will comprise of three main components – The first is a cloud backend service which will integrate provider's Electronic Health Record Systems (EHRs) for mobile app consumption called ***Locket Cloud***. The second is the ***Locket for Providers*** app which will improve provider's user experience when interacting with EHRs and the "consumability" of interrelated health data. The third is the ***Locket*** app which is targeted toward consumers. ***Locket*** will allow users to organize and actively manage their own health information.

2.0. Mockups and Wireframes

Using our User Centered Design (UCD) methodology which comprises of interviewing potential users, identifying user personas, defining information architecture based on the business needs of the solution, and following our mobile app design best practices, we have created the following mockups and wireframes of key screens and functionality within ***Locket for Providers***.

2.1. Mockups

The following mockups of ***Locket for Providers*** depict the look and feel of the mobile applications.

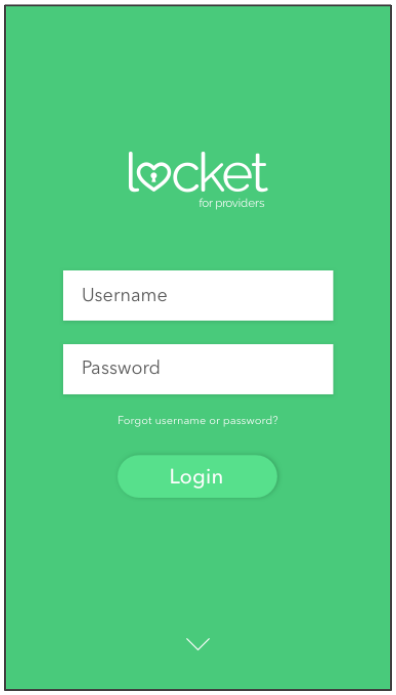
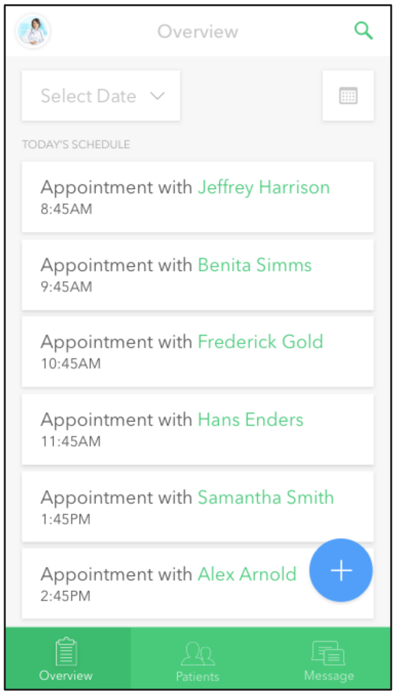


Figure 1: Each doctor's office will have a unique login to access patient health data.



Appointment with Jeffrey Harrison
8:45AM

Appointment with Benita Simms
9:45AM

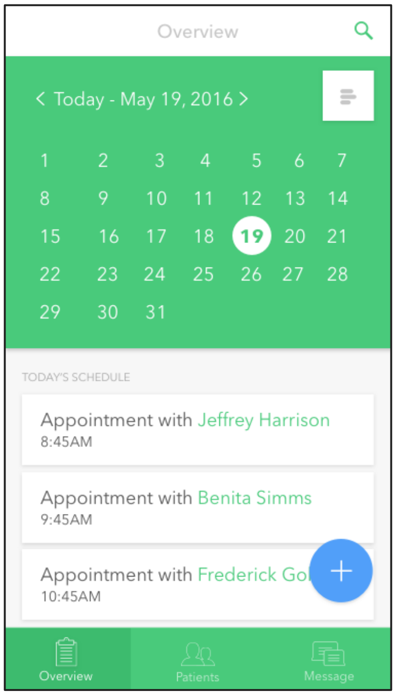
Appointment with Frederick Gold
10:45AM

Appointment with Hans Enders
11:45AM

Appointment with Samantha Smith
1:45PM

Appointment with Alex Arnold
2:45PM

Figure 2: The provider can access their schedule through a list format and receive alerts prior to the next scheduled appointment.

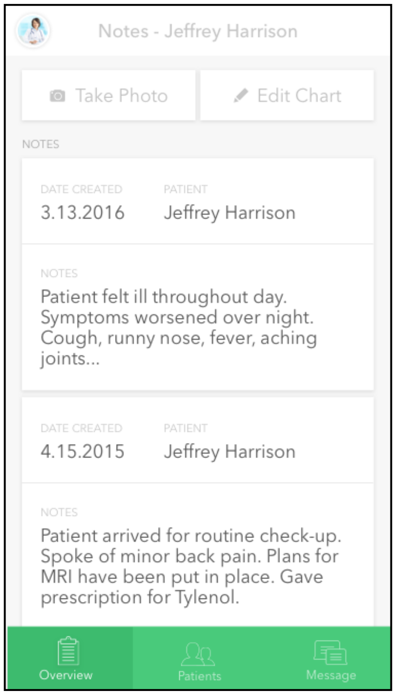


Appointment with Jeffrey Harrison
8:45AM

Appointment with Benita Simms
9:45AM

Appointment with Frederick Go
10:45AM

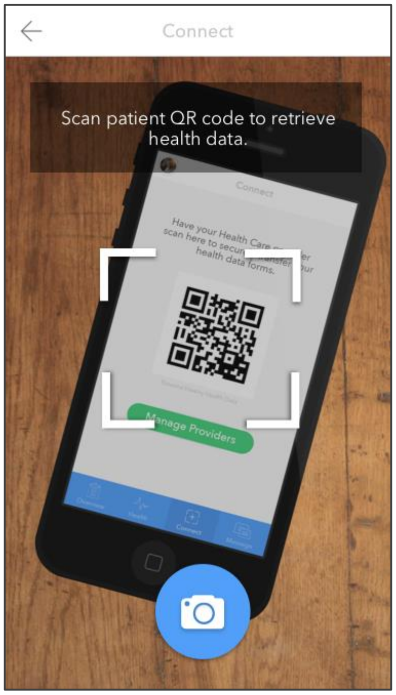
Figure 3: The provider can swap to a calendar view based on their preference for viewing upcoming appointments.



DATE CREATED 3.13.2016
PATIENT Jeffrey Harrison
NOTES Patient felt ill throughout day. Symptoms worsened over night. Cough, runny nose, fever, aching joints…

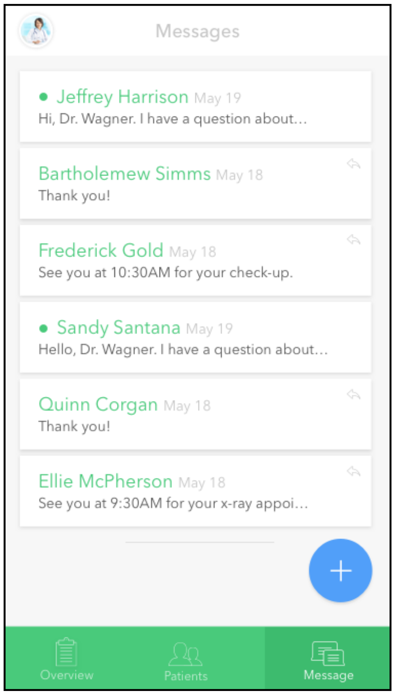
DATE CREATED 4.15.2015
PATIENT Jeffrey Harrison
NOTES Patient arrived for routine check-up. Spoke of minor back pain. Plans for MRI have been put in place. Gave prescription for Tylenol.

Figure 4: The provider can create custom notes during appointments manually or through the camera feature.



Scan patient QR code to retrieve health data.

Figure 5: The provider can scan the QR code from the consumer app to quickly access and store updated patient health data.



● Jeffrey Harrison May 19
Hi, Dr. Wagner. I have a question about…

Bartholemew Simms May 18
Thank you!

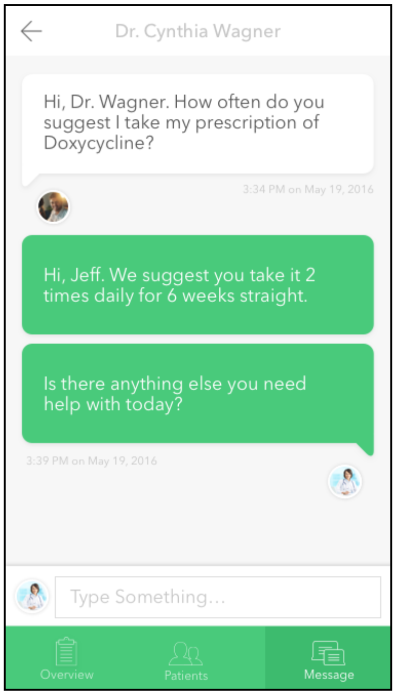
Frederick Gold May 18
See you at 10:30AM for your check-up.

● Sandy Santana May 19
Hello, Dr. Wagner. I have a question about…

Quinn Corgan May 18
Thank you!

Ellie McPherson May 18
See you at 9:30AM for your x-ray appoi…

Figure 6: The provider can get in touch with patients through the messaging feature.



Hi, Dr. Wagner. How often do you suggest I take my prescription of Doxycycline?
3:34 PM on May 19, 2016

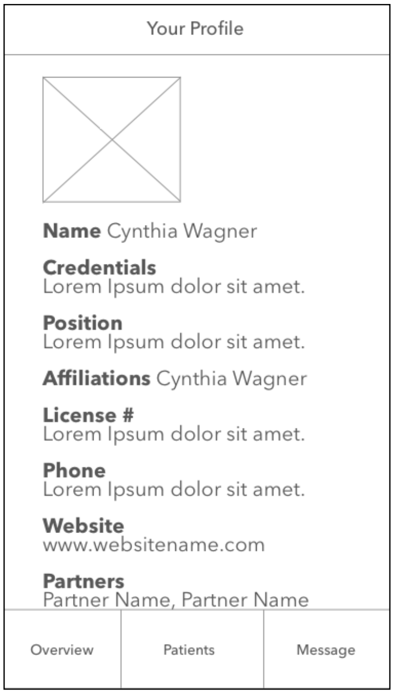
Hi, Jeff. We suggest you take it 2 times daily for 6 weeks straight.

Is there anything else you need help with today?
3:39 PM on May 19, 2016

Figure 7: The provider can get in touch with patients through the messaging feature.

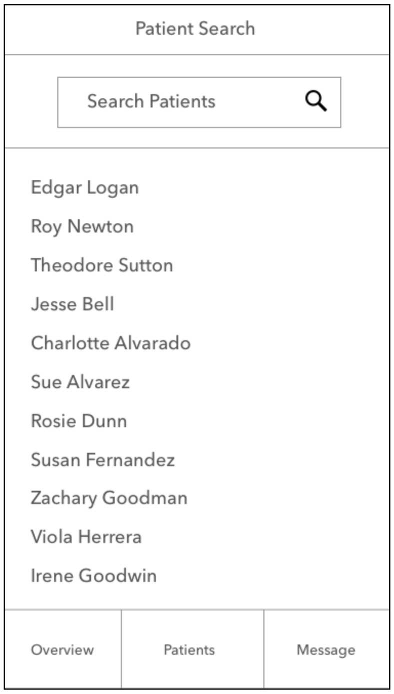
2.2. Wireframes

Wireframes depict the layout of UI components and determine the user-experience and information architecture of the app



Name Cynthia Wagner
Credentials Lorem Ipsum dolor sit amet.
Position Lorem Ipsum dolor sit amet.
Affiliations Cynthia Wagner
License # Lorem Ipsum dolor sit amet.
Phone Lorem Ipsum dolor sit amet.
Website www.websitename.com
Partners Partner Name, Partner Name

Figure 8: Provider profile screen.



Edgar Logan
Roy Newton
Theodore Sutton
Jesse Bell
Charlotte Alvarado
Sue Alvarez
Rosie Dunn
Susan Fernandez
Zachary Goodman
Viola Herrera
Irene Goodwin

Figure 9: Patient search screen.

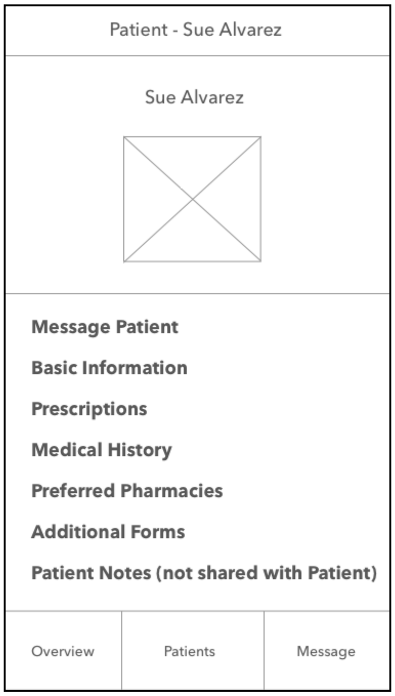


Figure 10: Patient profile screen.

3.0. Technical Specifications

3.1. Data Sources

MetroStar plans to integrate ***Locket for Providers*** with several of the top ten EHR systems, as measured by Meaningful Use attestation per HealthIT.gov, including EHRs from:

- Epic Systems
- Allscripts
- NextGen Healthcare
- Cerner
- McKesson
- Athena Health

Of these EHR Systems, Epic Systems, NextGen Healthcare, Cerner, and McKesson are part of the Health Level 7 (HL7) Argonaut Project. The purpose of the Argonaut Project is to rapidly develop a first-generation FHIR-based API and Core Data Services specification to enable expanded information sharing for electronic health records and other health information technology based on Internet standards and architectural patterns and styles. Epic Systems, Cerner and NextGen Healthcare are verified to have support for Fast Healthcare Interoperability Resources Draft Standard for Technical Use 2 (FHIR DSTU2). They will therefore be prioritized for implementation into ***Locket*** with minimal friction. Allscripts, and Athena Health do not implement a FHIR API but do implement their own APIs with varying degrees of functionality.

3.2. System Architecture

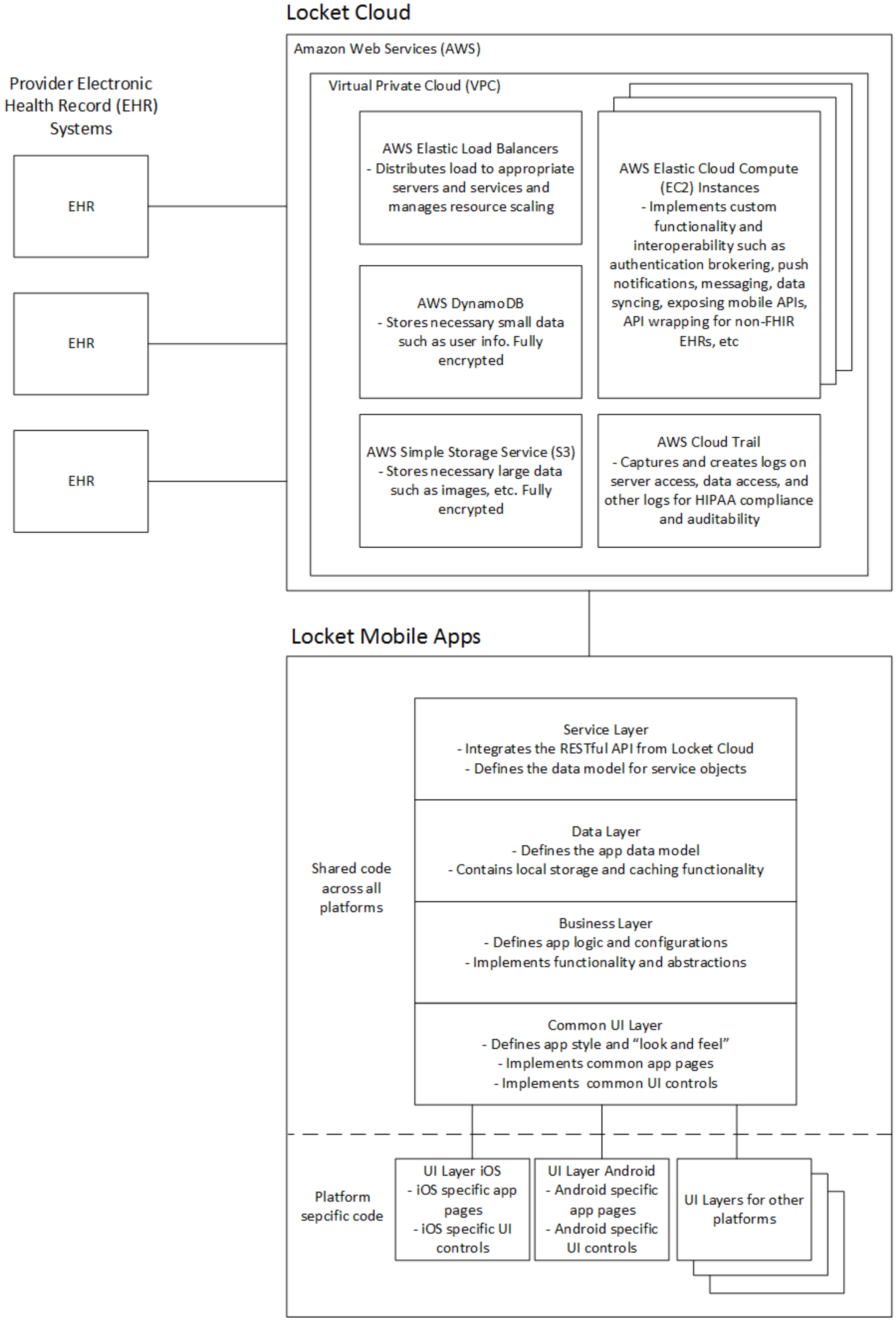

Locket Cloud
Amazon Web Services (AWS)
Virtual Private Cloud (VPC)
Provider Electronic Health Record (EHR) Systems
EHR
EHR
EHR
AWS Elastic Load Balancers - Distributes load to appropriate servers and services and manages resource scaling
AWS Elastic Cloud Compute (EC2) Instances - Implements custom functionality and interoperability such as authentication brokering, push notifications, messaging, data syncing, exposing mobile APIs, API wrapping for non-FHIR EHRs, etc
AWS DynamoDB - Stores necessary small data such as user info. Fully encrypted
AWS Simple Storage Service (S3) - Stores necessary large data such as images, etc. Fully encrypted
AWS Cloud Trail - Captures and creates logs on server access, data access, and other logs for HIPAA compliance and auditability
Locket Mobile Apps
Shared code across all platforms
Service Layer - Integrates the RESTful API from Locket Cloud - Defines the data model for service objects
Data Layer - Defines the app data model - Contains local storage and caching functionality
Business Layer - Defines app logic and configurations - Implements functionality and abstractions
Common UI Layer - Defines app style and "look and feel" - Implements common app pages - Implements common UI controls
Platform sepcific code
UI Layer iOS - iOS specific app pages - iOS specific UI controls
UI Layer Android - Android specific app pages - Android specific UI controls
UI Layers for other platforms

*Figure 11: **Locket** Cloud and Mobile System Architecture*

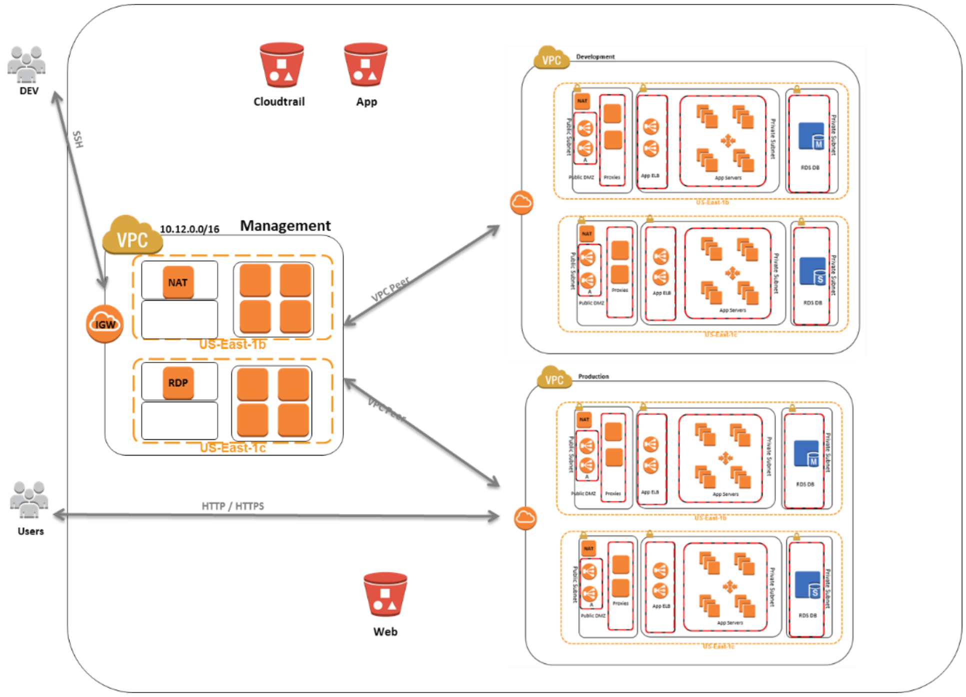


Figure 12: Standard 3-Tier Web Architecture for NIST on AWS with Optional Development and Management VPCs

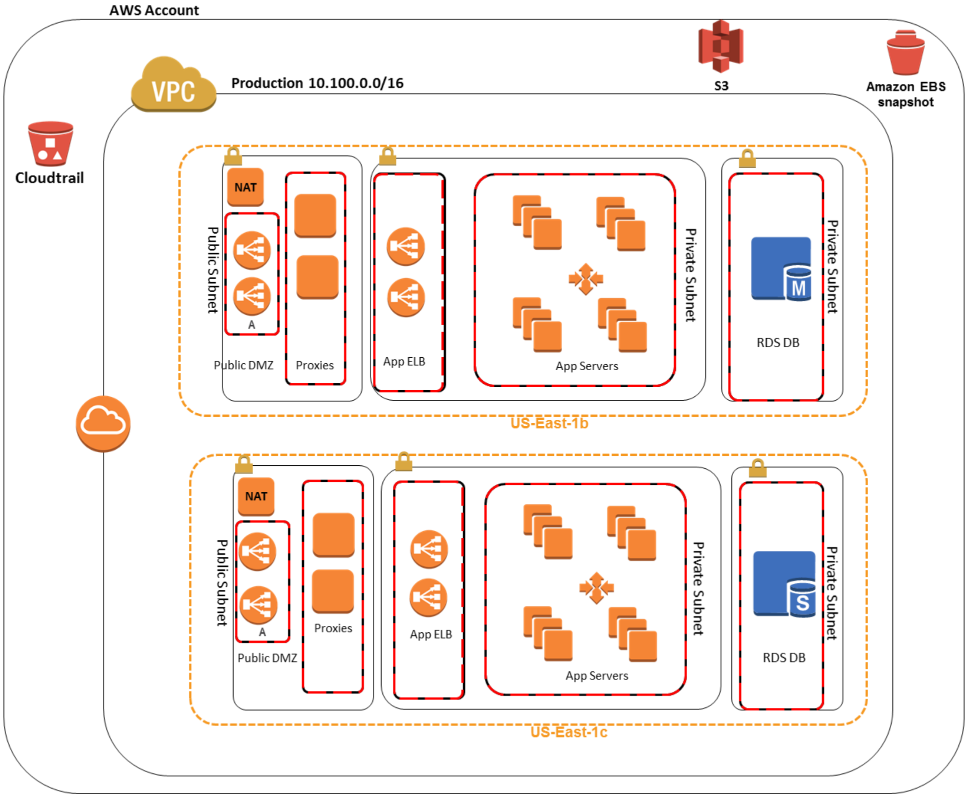


Figure 13: VPC Detailed Design for NIST on AWS

Locket Cloud will be hosted on an Amazon Web Services Virtual Private Cloud (AWS VPC). The backend will consist of AWS's Elastic Compute Cloud (EC2) service for custom functionality with Linux based applications, AWS DynamoDB Database for data storage up to 400KB, and AWS Simple Storage Service (S3) for files up to 5TB. The backend service will also utilize AWS Elastic Load Balancing (ELB) for managing scalability and performance. One of the biggest advantages of using the AWS cloud is that the ***Locket Cloud*** backend will be able to scale available resources up as needed to ensure high performance, and also down when necessary to maintain a low cost of operation. The ***Locket*** backend system will act as a middleware or intermediary between the EHRs and mobile apps. It will connect to the EHRs using secure VPN tunneling and to the ***Locket for Providers*** mobile application by exposing a Representational State Transfer (RESTful) Application Programming Interface (API) in a hybrid configuration. ***Figure 10*** shows the cloud and mobile system architecture while ***Figure 11*** and ***Figure 12*** show the server topology and configuration for the cloud service.

3.3. Mobile Architecture

The ***Locket*** mobile apps for iOS and Android will be built using the Xamarin cross-platform mobile development platform. This will allow us to maximize code reuse between all mobile platforms. Previous projects have shown up to 90% code reuse using Xamarin tools and reduced development time by more than half for subsequent platform releases. In addition to that, utilizing Xamarin will also allow us to release ***Locket*** for other major platforms including the Universal Windows Platform (UWP) which covers desktops, laptops, tablets, Windows Phones, and Xbox One, and also the Apple Mac family of devices which includes MacBooks, iMacs, Mac Pros, and Mac Minis. The mobile applications will be built with a layered architecture implementing the Model View ViewModel (MVVM) pattern for code decoupling and reuse.

3.4. Data Integration

Locket for Providers will allow users to sign in through the mobile app into existing EHR platforms using OAuth, Security Assertion Markup Language (SAML), or Single Sign On (SSO). The backend cloud service will broker this authentication to ensure that the user’s data can be synchronized and updated.

When the user has gained access to the EHR through the ***Locket Cloud***, they will be able to access their patient’s information covered in the Common Clinical Data Set if the EHR they are connecting to supports the FHIR DSTU2 standard.

For EHRs that expose partial or custom APIs, the ***Locket Cloud*** will wrap the API so that the transition from EHR to mobile application is seamless. However, if some of the data is inaccessible due to the different API model, the ***Locket Cloud*** will notify the app of the inaccessible data.

The ***Locket Cloud*** will expose a REST API with JSON to the mobile apps which will integrate the APIs using HTTP calls to the API. The apps will then deserialize the JSON to the relevant app data model objects.

3.5. HIPAA Compliance

To ensure compliance with HIPAA regulations and maintaining the privacy and security of all data and electronic Personal Health Information (ePHI) within the system, the cloud service will:

- Be hosted on an AWS VPC (Virtual Private Cloud) and only use HIPAA compliant AWS

services such as EC2, S3, DynamoDB, CloudTrail, and more. AWS aligns their HIPAA risk management program with FedRAMP and the NIST 800-53 security standard.
- Encrypt all data in rest and in transit using industry standard encryption.
- Log all data and service access using AWS CloudTrail for auditability and threat management.
- Access EHRs through secure Virtual Private Networks (VPNs) configured behind firewalls within the ***Locket Cloud***.

Locket for Providers and ***Locket***, on all platforms, will:

- Encrypt all data in rest and in transit using industry standard encryption algorithms
- Require authorization when the user accesses the app
- Provide alternative authentication methods and privacy safeguards such as pin numbers and biometric scanning per device hardware availability

4.0. Business Plan

4.1. Issue Analysis

It is hard to keep data secure, especially when data security is complicated and inconvenient. Not only is convenience important for healthcare provider satisfaction, it can also make healthcare providers better able to get the information that they need to make critical medical decisions. Fortunately, technology can provide a solution to some of the barriers healthcare providers face when giving care.

Healthcare providers have fragmented access to health data. Providers can be contracted to work at multiple locations—which means having to manage multiple logins, user interfaces, and types of patients. While it could be argued that another application would just create another sign on and interface to learn, the drawbacks could be outweighed by having a home base for all professional activity.

In hospitals, it is quite common for healthcare providers to be on call overnight. Having mobile access to patient health data on a hospital issued approved application could be useful if urgent decisions need to be made while a provider is on the phone with a less trained hospital staff member.

Antiquated forms of communication are expensive and hinder communication among specialists. Healthcare providers are prevented from emailing another provider about the details of a patient. While providers may pick up the phone to talk to each other about a patient, it is unlikely that chose this option. Health institutions have developed complex, inefficient ways to overcome the issue of providers not being allows to email each about patient data. Some healthcare systems fax information from one office to another. Others have a provider write a letter, print the letter, and physically send the letter to another institution. An online, secure system for messaging could save both time and money associated with communication about patient health.

Drug interactions kill four times as many people as traffic accidents. Healthcare providers have a job that is mentally taxing since the stakes are high their decisions complicated. Additionally, many of the technological tools that are implemented in the health systems do not have good usability. Therefore, they could use digital tools to augment their current workflow that demonstrate superior usability that comes from rigorous user testing.

Overall, healthcare providers need tools that better facilitate tasks like accessing patient data or communicating with external providers.

4.2. Solution Description

Locket for Providers aims to merge convenience and security when managing patient health data. Rather than replacing existing EHRs or other digital tools, the application will bring them all together to maximize ease of use.

While healthcare providers will still need to have multiple accounts with different health institutions, ***Locket for Providers*** will provide a central home for all professional information. Providers will have a direct way to communicate with patients, coworkers, and providers at different healthcare institutions through a secure messaging system. ***Locket for Providers*** natively integrates with the regular ***Locket*** app that consumers use. This allows for providers to leave digital notes to their patients. Providers can remind patients to take medications, update their prescriptions, and answer questions. No patient data is saved on the device and ***Locket for Providers*** needs a PIN or fingerprint to open even if the mobile device is unlocked.

Locket for Providers will allow peer to peer communication between providers at different healthcare institutions. All of the accounts will be verified, encrypted, and not leave the servers dedicated to ***Locket***. This peer to peer messaging system solves the issue of inefficient transfer of information. As long as both providers have the application, they can directly communicate about patients given sufficient permissions from their institutions. The messaging tool will become more and more powerful as more physicians adopt ***Locket for Providers***.

Even when on call, the provider can access patient information to inform a decision about a patient's health when away from the hospital. When in the office or on the go between patients, providers can choose to access patient data on the app. While ***Locket for Providers*** will probably not replace a desktop user interface for an EHR, but it could provide a flexible user friendly way to view patient information.

Locket for Providers will also streamline routine tasks, such as requesting prescriptions for patients. While there are already systems that can assist with writing prescriptions, the native integration will add value to the application by being the go to app for providers.

Locket for Providers should ease the workflow of healthcare providers while insuring the high level of security that health professionals require.

4.3. Financial Estimates

The development of this application will have a lower startup and maintenance cost due to the experienced developers at MetroStar Systems. The cost range for the development of the application is $200,000+, which is less than half of the market average price for an app of this caliber. Looking ahead, MetroStar also recommends a budget to evolve and enhance the native mobile app and its backend services by releasing new features and/or enhancements to the backend platform every three months over the course of one year.

4.3.1. Initial development cost

The initial development is estimated to take sixteen weeks or eight two-week sprints using MetroStar's agile development methodology. This will include the ***Locket for Providers*** app and ***Locket Cloud*** design, development, testing and deployment efforts. ***Locket*** consumer app development is discussed in the submission or the HHS Consumer Health Data Aggregator Challenge. MetroStar is fully equipped for the full lifecycle of development and deployment of cross platform mobile apps. Therefore, there will be no additional hardware or software costs involved.

Role	Hours	Cost per hour	Total
Project Manager / Business Analyst	320	$82.95	$26,544
Mobile Developer	640	$106.80	$68,352
Backend Developer – Cloud	640	$100.59	$64,378
User Experience Expert	320	$60.00	$19,200
Graphic Designer	320	$62.29	$19,933
Software Tester	400	$51.85	$20,740
Total			**$219,147**

4.3.2. Ongoing quarterly maintenance and development cost

We estimate quarterly maintenance and development to be carried out in two two-week sprints each for an estimated total of $54,786.75. Resources can also be appropriated for different tasks such as marketing, training, and additional EHR integration based on the evolution of ***Locket for Providers***.

4.3.3. *Locket Cloud* operation cost

Based on previous high availability cloud services that MetroStar Systems has built, using an initial estimate of one thousand users and the proposed cloud architecture, the AWS environment will require two proxy servers, one web application server, and one database server. Using generous estimates in the AWS Calculator, the monthly cost of operation is $644.42. Therefore, the monthly cost per user is estimated to be $0.65.

4.3.4. Revenue

Locket for Providers will utilize a subscription business model for a steady revenue stream which is common for Software-as-a-Service (SaaS). Providers will also be charged a relatively small fee for initial consultation, installation (integration with ***Locket Cloud***), and training materials. Pricing will vary from provider to provider depending on number of users and patients. MetroStar estimates the average for upfront cost will be in the vicinity of $10,000 with a yearly subscription fee of $6,000. Assuming a conservative growth rate of one provider per month and 100 users per provider for simplicity, ***Locket for Providers*** will break-even for initial development costs in 16 months and be profitable in 27 months.

4.4. Engagement Plan

Our first marketing strategy is to create a great product, ***Locket for Providers***, which is helpful and easy to use. MetroStar has a mature team for all stages of mobile development—user experience, graphic design, and cross-platform. To successfully reach critical mass MetroStar plans to gain acceptance in a few health systems before scaling at a national level.

One example of MetroStar launching a product is its subsidiary, Zoomph. Zoomph was initially launched as a project within MetroStar to help the White House moderate a twitter question and answer session. The platform was successful enough to launch as its own company. Not only has the creation of the Zoomph product and company shown that MetroStar can create a valued product, MetroStar also has a marketing collaborator since Zoomph specializes in promoting products on social media.

Before deployment, MetroStar will have targeted pilot tests. MetroStar's user experience philosophy is to test early and to test iteratively. The initial user tests will inform the design of the interface, the interactions, and the marketing strategies. Once ***Locket for Providers*** is developed internally and ready for deployment, it will continue to receive updates based upon the needs of healthcare consumers and health care staff. After introducing pilot groups to ***Locket*** and encouraging their use of the app, the pilot groups will expand via marketing campaigns at hospitals and medical providers who host the application.

The primary benefit that MetroStar can pitch to providers and health systems is the time savings and control that comes with using the application. If a health system implements the app, they can save money and time brought about by the ease of communication among providers, staff, and patients. MetroStar staff will contact healthcare institutions directly to arrange support of the application. The goal is to use the early adopters of the system to give feedback on the usability of the apps and to make them as easy to use as possible. After the early adoption phase, MetroStar will begin charging new health institutions to implement the software.

MetroStar team has the talent from a marketing and technical perspective to create a well-liked health product. Once the app overcomes "acceptance inertia", MetroStar will be able to turn ***Locket*** into another project like Zoomph.

5.0. Provider Partnerships

5.1. Sport and Spine Rehab

Sport and Spine Rehab provides state of the art comprehensive care by combining chiropractic, physical therapy, rehabilitation and patient education to eliminate symptoms, restore full function and promote a healthy lifestyle. Their highly qualified doctors provide care to a wide range of patients for a variety of musculoskeletal conditions. They operate seven facilities in Virginia and Maryland.

Sport and Spine Rehab has provided a letter of intent to partner and collaborate with MetroStar to develop, design, test and integrate ***Locket for Providers*** and ***Locket***.

SPORT & SPINE REHAB
CHIROPRACTIC | PHYSICAL THERAPY | REHAB
Work Better, Play Harder

Sport and Spine Rehab,

10805 Hickory Ridge Rd,

Suite 103,

Columbia, MD 21044,

May 25th, 2016

MetroStar Systems,

1856 Old Reston Avenue,

Suite 100,

Reston, VA 20194

Sport and Spine Rehab intends to partner with MetroStar Systems in the development of two mobile applications: one for healthcare consumers and another for healthcare providers. The partnership includes allowing MetroStar to request development and design feedback for both mobile applications and also to discuss the potential of integrating and testing the applications with Sport and Spine Rehab's electronic health record systems.

Sincerely,

Dr. Jay Greenstein

Digitally signed by Dr. Jay Greenstein
DN: cn=Dr. Jay Greenstein, o=Sport and Spine Companies, ou=CEO, email=drjay@ssrehab.com, c=US
Date: 2016.05.25 11:46:15 -04'00'

Jay Greenstein

CEO

drjay@ssrehab.com