Business Case for MyHealthRec.io API

Thoughtkeg Application Services Corporation

Thomas “Rick” Bell

Executive Summary

MyHealthRec.com is an enhanced Patient Portal Web Application using Modern Web Technologies for Front-End Design. It accesses a RESTful Web Services Back-End, MyHealthRec.io. The MyHealthRec.io API provides access to an extremely powerful micro-services architecture which support, among other services, FHIR as both client and server, DIRECT protocol messaging, and the services enabled by the HEART WG’s specifications for OpenID-connect, User Managed Access (UMA), and OAuth2.

This API will be leveraged by a Web App and from Android Mobile clients to enable Patients, and their Proxies, to control the movement of the health data, implementing a version of consumer-mediated exchange. The problems for Patients in controlling their healthcare data are real and MyHealthRec.io goes some distance in relieving some of the burdens that Patients and providers face, enabling real progress at secure, user controlled movement of healthcare data.

This document also contains financial and implementation details that should support the viability of this project along with projections that suggest long term financial sustainability and ever prosperity. The MyHealthRec product presents value to the Patient in the form of pain-relief from the frustrating failures of a disconnected healthcare IT infrastructure. It presents value to the Provider, who seeks to improve patient experience, in the form of support in addressing the regulatory financial incentives brought forth with the recent MACRA legislation and the MIPS program. This value proposition should make the product attractive to both key parties, Providers and Patients, in this arena.

The Problem for Patients

As Patients navigate the healthcare system, they will often interact with several healthcare providers like doctors, hospitals, labs, imaging center and specialists. Though in recent years many providers have implemented electronic health records (EHRs), communicating between providers with different brands of EHRs is still done with faxes and telephone calls. Patients and their loved ones spend far too much time in provider waiting rooms filling out the same registration forms and giving the same history and physical information, to the best of their recollection.

Worse than that, far too often they have to hand-carry paper referrals, orders and reports between providers to assure that their information is successfully exchanged from one provider to another. And when the patient loses a paper document like a lab order or a referral, in some situations, the patient has no choice but to return to the ordering provider to have the document re-written. That can be very frustrating and an expensive waste of time off of work, fuel, etc.

The potential for problems is multiplied for individuals in the “Sandwich Generation”, adults ages 40 to 59 who have a parent 65 or older and raise a minor child or support a grown child. These individuals are the emotional, financial and logistical support for loved ones, where logistical support often includes arranging trips to healthcare providers and curating provider paperwork. “Sandwich Generation” adults face the problems of navigating the healthcare system several times over.

The Problem for Providers

Providers already want to provide the best care for their patients and make the healthcare experience as smooth and easy as possible. Providers have struggled with meeting Meaningful Use Patient Engagement measure in part due to “multiple portals” problem, where patients have different usernames/password the portal provided by each provider (and it is even worse for “Sandwich Generation” adults.) Very few Providers would argue against streamlining the new patient registration process which is necessary but a chore for many new patients.

The recent The Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) legislation puts the majority of providers who see Medicare patients under the Merit-Based Incentive Payments (MIPS) program which includes monetary incentives for adopting technology to support patient access to health information, patient engagement, care coordination, and interoperability. And, there are escalating penalties up to four eventually nine percent per year of Medicare revenue for those who do not.

Therefore, is it not difficult to imagine that Providers would be receptive to a patient-centered solution that makes navigating the healthcare system easier for their patients and helps them address regulatory incentives.

The Solution

The “Sandwich Generation” especially, but all individuals navigating the healthcare system generally, would benefit from a solution that keeps healthcare paperwork as data and enables the secure motion of that data between providers with minimal risk of loss, theft, or corruption. Furthermore, there would be benefit from individuals having the ability to define explicit rules about who can access their data and what can be done with that data. Delivering a solution like this on the web and on mobile devices is exactly the goal of the MyHealthRec.com web application and the API on MyHealthRec.io, respectively.

The MyHealthRec.io API will provide the Patient with a capability to set, enforce, and monitor policies controlling the access and movement of their healthcare data as described in the HEART Working Group’s (HEART WG) specification for User-Managed Access (UMA), especially. There are several key points in navigating the healthcare system where MyHealthRec.io can assist patients with managing the movement of their data: registration, referrals, and sharing orders and results or reports. Putting the Patient, and their support system (often a member of the Sandwich Generation), in control of their data will relieve some of the headache and frustration of navigating the healthcare system.

For the Patient using the MyHealthRec.com web application, the experience would be much like most Patient Portal web applications, where the patient can review summaries of recent visits, results/reports, and messaging, with a few enhancements. Most notably, the Patient can visit a user-interface screen and identify other users to be allowed to view specific data or documents.

Expanding this idea, the Patient could indicate which users can see certain types of data or documents. Further, the Patient could indicate that certain types of users are allowed to see certain types of data or documents. For example, a Patient could indicate that “Any User identified as my Primary Care Provider can view all of my documents” and “Any User identified as my Specialist Provider can view all of my documents, except for my lab results for STD testing and substance abuse.” Correspondingly, a Provider could control what data is released to them by indicating something like, “this Provider will receive demographics, history and physical, and only results from tests order by this Provider.” Furthermore, if the Patient is not as facile with technology, he or she can delegate sharing authority to their Proxy. And this is just the start of what kind of controls and workflows are possible. When the policies, or sharing rules, are set up for a Patient, sharing data can be user-friendly and even automated.

The API can also assist with the new patient registration process, assuming the Patient already is registered with MyHealthRec.io and the new Provider’s EHR is enabled as a FHIR Client, the Patient, upon presenting at the Provider’s office, could log into her phone and then present a Quick Read (QR) barcode for the registration clerk to scan. That scan could make the Patient known to the new Provider’s practice (and registered in the new Provider’s portal.) And it would enable the new Provider’s EHR to securely pull demographics, history and physical, referrals and recent results data. This would make registration at a new provider more like boarding a plane recently. Behind the scenes, the flurry of interactions would be complex, but the experience for the patient would be streamlined.

For Providers, the MyHealthRec.io API would assist in meeting the Application Access (API) 2015 edition certification criteria because the API provides access to a FHIR Server which can take authorized request from a FHIR Client. And the MyHealthRec.io API would assist with the View, Download, and Transmit to a 3rd party, Secure Messaging, and Transitions of care certification criteria by, itself, providing access to another API supporting message exchanges over the DIRECT protocol. In the past, these criteria have posed some of the greatest difficulty for Providers and Health IT Vendors, but challenges should be met comfortably going forward. With those challenges addressed, Providers should have few worries regarding the Health IT aspects of the MIPS program and be in position to benefit rather be penalized.

Methods and Technologies for Solution Development

Thoughtkeg Application Services Corporation (TASC) primarily focuses on software development in the web application, web services and business intelligence space. For the project in discussion, the main objectives will be to develop a RESTful Web Service to serve as an API, MyHeathRec.io, that supports a web application, MyHealthRec.com, and an Android Mobile Application, likely to be named something like the MyHealthRec.com App.

The MyHealthRec.com web application will be a Single-Page Application (SPA) written on HTML5, CSS, Javascript (ECMAscript 6) using Bootstrap, a responsive web framework. The web application would be accessible on laptops, tablets, desktops, and phones through their browsers that handle HTML5, etc. The web application will focus on user interface design, because transactional processing and handling data will mostly take place through MyHealthRec.io API on the back-end servers. The web application will take a good deal of inspiration regarding design from the showcase at www.healthdesignchallenge.com.

The MyHealthRec.com App will be an Android mobile app developed using Android studio. The mobile app will focus mostly on the user interface design, because transactional processing and handling data will mostly take place through MyHealthRec.io API on the back-end servers.

The MyHealthRec.io API will be developed at its core using several of the Apache Software Foundation's projects: Tomcat (Web App Server), ServiceMix (OSGi), CXF (Web Services), Oltu (Oauth2), Camel, Commons. Object-Relational Management (ORM) will be handled with Hibernate. Back-End development using encryption will be done with the Bouncy Castle Crypto API's. The FHIR Client/Server development will use the open-source project HAPI-FHIR. One can recognize the Java-centric approach which is not unusual for enterprise development, and the project also benefits from having so many key components already developed. The MyHealthRec.io API itself will leverage identity management API's for OpenID-Connect and Oauth2 provided as a service from Auth0. DIRECT messaging API's will be provided by Nitor Group's HISPDirect. The relational database management system (RDBMS) used will be PostgreSQL.

TASC will be presented with an important choice on how to implement the HEART User Managed Access (UMA) specification. Either TASC will start with ForgeRock's OpenAM (OpenUMA)open source implementation or TASC will elect to use the UMA spec and build on top of Apache Oltu, which is an implementation of Oauth2. TASC expects that implementing the UMA spec will be one the most challenging aspects of the project

TASC is able execute its objectives in a capital efficient manner because of the use of open source software and the hard work contributed to the community by other developers. And TASC looks forward to contributing back to the community as the project proceeds.

Financials

The MyHealthRec.io API project is one of the first projects for Thoughtkeg Application Services Corporation (TASC) which is a digital health startup launched by Thomas "Rick" Bell. TASC provides Software as a Service (SaaS) products and consulting services in the healthcare IT arena. Rick Bell has funded TASC with an initial $115k initial investment. The initial investment will be allocated to fund development and launch of health IT products and services. Rick Bell, himself, will subsist on savings as TASC ramps up. In addition to his initial investment, Rick will pursue seed capital through angel investors, micro venture capital firms and, potentially, equity crowdfunding sources.

Below is the expense budget for the MyHealthRec.io project showing the costs to develop, certify and launch the product. Making an assumption that over 2017 there will be 125 providers onboarded each with a large panel of 2000 patients, the associated hosting and subscription costs for that capacity are listed as well. Please note that the cost of hosting and subscriptions represents a high-water mark. Those costs are somewhat commensurate with the number of providers and patients on-boarded, so in the early months where the system sizing needs are lower, there will be lower costs. However, for expense projection purposes an average monthly rate will be used.

MyHealthRec.io API Project Budget – 1 Year Cost thru 2017	**Cost**
Web Front Development Tools	~2,500
Apache Software Foundation Open Source Software	0
2015 Edition Health IT Certification Modules ICSA Labs	~20,000
User Experience Evaluation	~8,000
Security Consultant Evaluation	~5,000
Development Consulting as needed	~10,000
Other Application & Legal Support as needed	~10,000
Initial Development Costs	**~$55,500**
Amazon Web Services EC2 & Storage Hosting	~10,000
Auth0 Identity Management Solution, Multi-Factor	~5,000
F5 BIG-IP VE, Performance/Security Network Edge Software	~5,000
Nitor Group Direct HISP	~6,000
125 Providers/250k Patients(Proxies) **SaaS Hosting Cost**	**~$36,000**
2017 Project Costs Total	**~$91,500**

The schedule that follows is a revenue and expense projection covering the first year of operations concerning the MyHealthRec.io API project. The revenue assumptions made here involve the rate of providers adopting the solution and at a price point of $100 per Provider per Month. The provider adoption projections forecast results from a solo salesperson leveraging inbound marketing and customer relationship management tools as well as referral networking groups within a densely populated region, Southern California's Los Angeles, Orange, San Diego, San Bernardino, and Riverside Counties. The price point is a competitive with other patient portal offerings from Ambulatory EHR's, but will be reviewed as adoption data is gathered. This schedule is significantly simplified by omission of churn rates, sales promotion/discounts/sales team expansion, marketing efforts, business partnerships, and the impact of additional seed capital on sales and marketing efforts. However, the basic point should be clear that this solution's revenue can grow faster than the corresponding service delivery and sales costs expenses. Because cloud hosting and sales costs have been driven down dramatically in recent years, a well-developed service that benefits Patients and Providers at competitive rates will find not only sustainability but profit.

*Note that the first two columns show four months each, in contrast to the last four columns which each show only one month.

Projected Revenue/Expenses	Jan 2017 to Apr 2017	May 2017 to Aug 2017	Sep 2017	Oct 2017	Nov 2017	Dec 2017
Avg. No. of Providers per Month	8	20	40	65	95	125
Revenue ($100 Per Provider Per Month)	3,200	8,000	4,000	6,500	9,500	12,500
Hosting Expenses	16,000	16,000	4,000	4,000	4,000	4,000
Sales Costs	2000	2000	500	500	500	500
Gross Profit (Loss) (Rev. – Exp.)	**(14,800)**	**(10,000)**	**(500)**	**2,000**	**5,000**	**8,000**

Timeline

MyHealthRec.io API Project Timeline September 2016 through May 2017						
Track	Sept 2016	Oct 2016	Nov 2016	Dec 2016	Jan 2017	May 2017
MHDFC	Phase 1 Proposal Deadline				Phase 2 Prototype Deadline	Phase 3 Scale Deadline
MyHealthRec.io API Develop, Test, Certify, Launch	Front-End Development w/ Mocked Services. Identity Services Integration (OpenID-Connect & Oauth2). HIPAA & Risk Mgmt. Review.	HEART Profile specifications implementation (UMA & FHIR UMA as available). Interoperability Services Integration (DIRECT, FHIR, EAI). Back-End Service Development.	Integration, User Acceptance Testing. User Experience Evaluation. Web Security Features Implementation.	Prioritized Issue Resolution. Bug Fixes and Enhancements to support certification then Beta Launch. Security Evaluation.	January 9th, 2017, **Beta Launch** of MyHealthRec.io API and MyHealthRec.com Patient Portal application.	April 17th, 2017, **Production Launch** of MyHealthRec.io API and MyHealthRec.com Patient Portal application.
ICSA Labs	Initial Certification Registration & Introductory Calls	Finalization of Certification requirements to be tested.	Additional discussion regarding certification requirements.	2015 Edition Certification Testing		

Success Metrics

Though the primary customer segment is an adult who acts as a proxy and provides support for both an elderly adult and a child because these individual most acutely experience the burden of managing healthcare data between providers, however many types of patients experience some aspect of these pain points. Thus, it is important to measure growth the network of Patients, Proxies, and Providers with the following metrics:

Number of Sign Ups: Patients, Proxies, Proxy with 1+ Patients connected, Providers, Provider-Office-Staff
Number of Patients Known (Registered) to Providers, Providers Known to Patients(Proxies)
Avg. # of Each Type of Relationship

Once the MyHealthRec.io API is connecting Patient and Providers, it become useful to measure the utilization of the network through their participation in the network and success or failure:

Monthly Active Users: Patients, Proxies, Providers (& Office Staff)
Number of Data Sharing Patient Authorized Data Sharing Policies setup: Attempted/Successful
Number of Patient registrations done through MyHealthRec.io API using Policies: Attempted/Successful
Number of Care Summaries Shared: Providers to Patient(Proxy); Attempted/Successful
Number of Referrals, Orders, Results, Reports that are shared Provider to Provider using Policies; Attempted/Successful
Number of Data Sharing Transactions authorized individually and not by Policy
Customer Support Issues Raised by Role (Patient, Proxy, Provider), Transaction

Risks & HIPAA Concerns

Because MyHealthRec.io handles electronic protected health information data generated by a Provider who is a covered entity, Thoughtkeg Application Services Corporation (TASC) is a business associate and needs to enter into a Business Associate Agreement (BAA) with the Provider. As required, TASC agrees to comply with HIPAA requirements (Risk Management and Administrative, Technical, and Physical Safeguards, etc.). TASC must also investigate, report and respond to potential data breaches. Additionally, subcontractors of TASC must also enter into BAAs and as such TASC will seek BAAs with Amazon, Auth0, and Nitor Group. TASC will review with counsel on the need to seek a BAA with F5 because F5 provides Network Edge Technology and may fall under the "conduit" exception because F5 technology might not store PHI in the course of supporting application security and performance.

Through the MyHealthRec.io API, the patient is empowered to access (view/download) and direct (transmit) their information in accordance with HIPAA. This would include the fact that the Patient has the right to direct their information to a third-party of their choice. The patient is even allowed to use non-secure methods of transmission (like email) as long as they are warned and accept the risks. In the course of this project, the Patient will be further empowered to set up rules and policies that govern access to their information. TASC will take special care to review with counsel how authorization policies utilizing HEART WG's UMA spec align with HIPAA. To forecast, there is no obvious conflict or challenges, but TASC will be mindful as the implementation proceeds.

Patient health data managed by the MyHealthRec.io API is an attractive target for cyber criminals, hence a number of security measures, best practices and technology will be implemented. TASC will review and address the Open Web Application Security Project's (OWASP) Top Ten web application security flaws and Top Ten Proactive Security Controls as they pertain to MyHealthRec.com, the patient portal web application front-end, and the MyHealthRec.io API. TASC will address mitigation for the types of attacks on OAuth2 identified by SANS Institute and by the Internet Engineering Task Force (IETF) in RFC 6819. TASC will also use F5's BIG-IP technology monitor external access to the application to mitigate the threat of external attacks from the web. Within MyHealthRec.io's back-end, server to server communication will use Transport Layer Security (TLS) and all PHI will be de-identified or encrypted at rest. Additionally, access to all servers by system administrators will require Multi-Factor Authentication (MFA). Finally, TASC will engage a GIAC Certified Web Application Defender to evaluate the MyHealthRec.com web application and the MyHealthRec.io API. The sum total of these measure should do well to mitigate the known cyber threat, nonetheless TASC will continue to monitor and stay current as threats evolve.

Participants

Thomas "Rick" M. Bell, III, Founder and CEO of Thoughtkeg Application Services Corporation (TASC) will serve as full-stack CEO on the MyHealthRec.io API project. Rick has recently left his IT Director position at Pomona Valley Hospital Medical Center to launch his own venture in the Health IT space. Rick has direct experience with the ONC Health IT Certification process, the development of successful Patient Portals, and has successfully led efforts for Meaningful Use Attestation. Rick has broad experience with systems integration, developing and using web services using open-source software, and business intelligence. He is a Sun Certified Java Programmer from 2001, and an Oracle Certified Database Administrator from 2003. He was the developer for Pomona Valley Hospital's ONC Certified patient portal as identified in the ICSA Labs certification notice, https://www.icsalabs.com/sites/default/files/2014-EHRI878950-2014-1027-00.pdf, with which Pomona Valley successfully attested for Meaningful Use.

TASC will also rely on the resources of the following companies to deliver the MyHealthRec.io API: Amazon Web Services (Cloud Hosting), Auth0 (Identity Management – OpenID-Connect and Oauth2), F5 (Network Edge Performance and Security Technology), Nitor Group (DIRECT HISP).

TASC anticipates working with Pomona Valley Hospital Medical Center and several Southern California providers, but those relationships have not been formalized.