Executive Summary

Informed Health Technologies, Inc. (IHT) is pleased to submit the Medical Hub® for your consideration in the Move Health Data Forward Challenge sponsored by the Department of Health and Human Services. The Medical Hub® is a care collaboration platform designed for secure sharing of health data following the HEART WG recommendations.

Until a more accurate term than 'patient' becomes available to reflect the diverse nature of individuals who want the ability to curate and share their health information, we will continue to use that word herein. The Hub, however, is being designed and intended to serve the needs of all such individuals, not only those historically called patients.

We will also refer to Hub owners and Hub guests, so as to differentiate two individuals who are sharing data, both of whom have a Hub account. Hub guests have an ongoing connection to Hub owners with permission to view and, with additional permission, to enter information (such as vital signs obtained manually in the home) into the owner's Hub. Hub owners also have the ability to push health data to providers willing and able to accept it.

The Hub solves several health system challenges, most notably limited health data sharing and helping to achieve the elusive Triple Aim. By giving patients control over the aggregation and curation of their health data, health data sharing is no longer restricted by provider or vendor policies. Patients can share their health data in real time or push interval data to those health providers who are prepared to accept it.

Further, by expanding the care team to caregivers and others in the patient's social network, significant effort can be off-loaded from the health system to family members, friends, or neighbors who are interested in being more involved and aware, and who can become responsible for early interventions. These less acute interventions, like reminding an aging parent to get on the scale to obtain a weight, ultimately avoid ED visits and hospitalizations (including readmissions). Early interventions are less costly and more effective than late ones, supporting better health, better quality of life, and lower health system costs.

There are two primary types of Medical Hub® accounts, patient and provider. Patient accounts enable the collection, storage, and sharing of personal health data (similar to a PHR), clinical data (from EHRs), and device data (such as a wireless enabled scale). Patients may enter data directly or capture data from elsewhere. There is a secure messaging platform integrated into the Hub (HubMail) that enables patients to interact easily with their social network and their clinical care team. Key to the success of managing the patient's health status is the automatic generation of alerts sent to the patient's care network, both social and clinical contacts. In addition, providers have access to a graphical dashboard with all of their patients and can drill down to individual patients needing additional support or focused intervention.

The patient's clinical care plan is collected into the Hub and integrated with a rules engine that monitors performance of individual care plan items. The Hub identifies two types of clinical problems: dangerous clinical trends and failure to perform care plan recommendations.

Contact information (phone, text, email, HubMail) for each person in the patient's network enables the Hub to reach out to caregivers (personal and professional) according to the rules defined by the care plan. Patients are ranked by health status so that those needing more immediate attention can be quickly identified from the graphical dashboard available to providers and targeted for additional support. We believe that this comprehensive approach will minimize workflow disruption in the clinical environment in reaching that 'last mile' into the patient's home and be more acceptable to clinicians, more effective for organizations, and less costly overall.

A patient may obtain a Medical Hub® directly or on the recommendation of a clinical provider. The patient selects a username, password, and HubConnect Phrase. Though the Hub acts like a social network, to ensure patient privacy, there are no functions that enable someone to see who else is in the network. In order to connect to another patient, one must know the name and HubConnect Phrase of the person with whom a connection is being sought. This information must be shared by the patient outside of the Hub.

Furthermore, different from most existing social networks, the Hub supports one-way connections. A Hub owner may invite a Hub guest to gain access to their Hub data. This invitation is one way. If accepted, it will not permit the Hub owner to have access to the guest's Hub. A separate invitation is required for those cases where bidirectional sharing is desired. Consider that many, if not most, connections with someone who is ill will be to support the person who is ill. Each patient has the ability to control which categories of information will be shared with Hub guests. Each patient has the ability to request their health data from their clinical provider.

At this time, we are developing the ability to package CCDA content for delivery to providers. At the same time, we recognize that there is work to be done with organizational policies and procedures to enable provider organizations to accept this data.

Solution

The Medical Hub® uses a web services approach to provide patients access to their health data on secure IHT servers distributed geographically. Patients and providers may access the Hub on any device that will support a web browser, including phones, tablets, and televisions. Patients retrieve their health data from provider EHRs using the OAuth 2.0 authentication protocol. At this time, not all vendors or providers have the same view of access token duration. Access tokens are renewed prior to expiration, when allowed. OpenID Connect will be available, but not required, to ensure flexibility. Hub owners have the ability to give Hub guests granular access to either view or add data, supporting UMA.

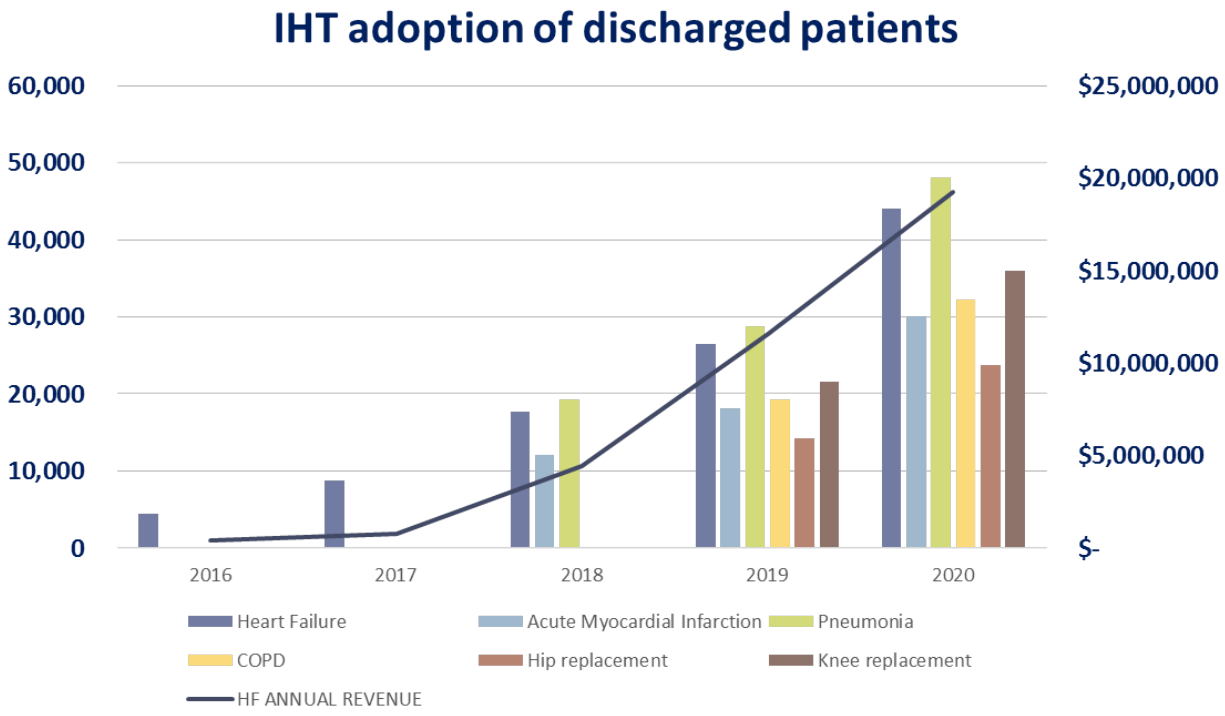
Financial overview

To date, the company has raised funds from the founder, friends and family. Costs have been optimized by balancing available resources with speed of development and minimizing non-development costs (to about 15%). For example, occupancy costs have been kept under $500 monthly. The founder is also an angel investor and will be pursuing additional investors once the next key milestone (EHR connectivity) has been achieved. Funds received will continue to be spent on development (about 30%), but spending will be expanded to growing infrastructure (e.g. server redundancy), managing a beta implementation, marketing, and sales.

The initial customer base will be hospitals working to avoid the Medicare 30-day readmission penalties. This market is easily identified from publicly available Medicare data. The measured population costs hospitals and healthcare systems millions of dollars in penalties annually ($420 million in 2015).

The first condition targeted will be Congestive Heart Failure (CHF). There is a high level of interest in a solution that removes or reduces financial losses associated with CHF.

Accuracy of financial projections by early stage companies is generally limited due to the large number of unpredictable factors. If execution on our plan is successful, competitors expand as predicted, health policy continues down the current path, and needed funding is obtained, the following chart shows plausible revenues projections.



The inflection points in the revenue projection recognize two expectations. For the first, we expect to build on demonstrated success with individual hospitals and have the ability to sell into large multi-hospital systems, which accelerates the adoption rate. For the second, we expect to expand our support for clinical conditions, rapidly increasing the patient population served for existing customers.

Development plan and timeline

The HIPAA compliant Medical Hub® platform, including the rules engine, has been built. The product is available on all devices supporting a web browser with https, from a smart phone to a television. Development is now focused on bug fixes, incremental upgrades, EHR connectivity, device connectivity (through third party APIs), and beta testing.

Bug fixes and feature upgrades are expected to be ongoing for the product's entire life cycle. Successful completion of EHR connectivity cannot reasonably be predicted. This is because it is not yet known if technical connectivity to an EHR vendor will be adequate to connect to all providers using that specific vendor or whether there will be nuances related to provider policies or implementations that will only be learned after making each new attempt to connect, requiring adjustments for each provider. The effort required cannot therefore be predicted. Device connectivity development will begin after additional funding is received and customers are imminent in order to minimize the cost of using third-party APIs prior to revenue generation. Beta testing is currently in negotiation.

Measuring Success

As a data driven solution, there are many metrics we are using to measure success. These measures will change over time as the product matures and adoption expands. In the early phase of the product we plan to measure:

- number of Hub owners
- number of shared Hub connections
- number of participating providers
- number of client hospitals
- number of alerts
- response time to alerts
- revenue

In the maturing phase of the product, we plan to additionally measure:

- profit
- client cost savings
- reduction in ED use, hospitalizations and 30-day readmissions compared to baseline

Risks

We have a risk document that is, in itself, 5 pages, not including mitigation strategies. As such, there isn't space herein for a complete consideration of risks, so we have focused on a key subset therefrom.

We pay a lot of attention to privacy and confidentiality, and many safeguards are built into the product. IHT staff do not have access to any Hub without explicit permission from the Hub owner. There is no central global override or golden key. Unfortunately, nothing can be done to prevent customers from writing down and sharing their passwords.

Security is an ongoing issue (like fixing bugs). There are huge incentives for theft of health information, leading to health data being under constant attack looking for weaknesses. To mitigate this risk, our system is Unix-based, which historically has tended to be harder to breach when properly configured (which we believe our servers are). Each patient has a separate, encrypted database. Code injections should not be possible as every web form strips unwanted characters before being processed. Direct changes to URLs can't lead to another owner's Hub. Each login creates a new, time-limited token. This token is refreshed when an action is taken and becomes invalid after a set period of time. If access using this token is attempted from a new IP connection or the token is outdated, the token is invalidated, logging out both the cracker and the Hub owner, forcing a new login. Hub guests can only visit pages that have been authorized. This authorization is verified each time a page is loaded. Hub guests without edit permissions cannot enter data into an owner's Hub.

While not a mitigation strategy, attempted reparations have been commonly employed for major security breaches among health plans like Blue Cross. In the event of a breach, we would have adequate insurance in place to support the needs of patients and offer credit monitoring services at no cost. However, in many cases it will be dependent upon the individual to monitor their own EOBs watching for services they did not obtain. As a result, an educational outreach effort would also be undertaken.

There are operational risks ranging from competitors beating us on features and price, to lack of customer interest, to running out of money. At the forefront of these risks is insufficient capital. The other risks occur only after we go to market. Our near-term goal is to raise sufficient funds to support our beta testing and early sales efforts to get to the point of positive cash flow. Our team is very experienced in healthcare and information technology, so we are confident that we will observe key trends regarding these challenges with enough time to execute our mitigation strategies.

Leadership Team

We are fortunate to have seasoned healthcare leaders on the IHT team.

Larry Ozeran, MD, Founder and President, has been a programmer, database administrator, general and trauma surgeon, and health organization leader for more than 2 decades. He has served on most hospital and medical group committees, including separately on the Board of Directors of a medical group and a hospital. He has been deeply involved in health policy at the state and national level, spending 2 years on the AMIA and HIMSS public policy committees. He has responded to several federal NPRMs. Dr. Ozeran is responsible for setting strategic direction in collaboration with Ms. Watman and IHT advisers. He also manages finance, personnel, and technical decisions.

Melinda Watman, BSN, MSN, MBA, Chief Operating Officer, spent 15 years as a clinician before obtaining her MBA and transitioning to entrepreneurial endeavors. She has successfully worked with both startups and established companies taking innovative healthcare technologies to market with noteworthy financial returns. One such endeavor resulted in a $45M recurring revenue stream in 3 ½ years. Melinda also has extensive experience operationalizing processes for improvement and growth resulting in enhanced performance and revenues. Ms. Watman is an active member of the New England Chapter of HIMSS and the New England Healthcare Executive Network. She is responsible for operations, sales, and marketing.

Alfredo Czerwinski, MD, Advisory Board Chair, is an MIT graduate who worked in Operations Research and Management Consulting before training in Internal Medicine at UCSF and UCLA. He has served as Corporate Medical Director at Kelsey-Seybold Clinic, Chief Medical Officer for the Sutter Health system, and CMO at CareScience. As a consultant, he is privileged to serve senior leaders in health care and information technology across the country.

Sherri Cherman, PharmD, Advisory Board Member, is a strategic and seasoned leader of high-growth organizations providing Specialty Pharmacy and Specialty Infusion services nationwide. A driver of vision and company performance, she excels at solving deep-seated business challenges, developing startup businesses, and leading growth opportunities in accretive mergers and acquisitions.

Aaron Day, Lead Developer, is a graduate of CSU Chico with a degree in Web Technologies & Services. He has 8 years experience as a full stack developer with increasing responsibility and has been in the health IT space for 6 years, including 5 years at UC Davis.