Dartmouth Secure Biometrics

Marketing Plan for Biometric Bracelet

Engineering & Technology Management
ETM 555/655 Spring 2013

Dr. Antoine Jetter

Portland State University

Team #3-
Elizabeth Gibson
Ignacio Castillejos
Joseph Lethlean
Kruti Narvekar
Kshiti Shah

Table of Contents

1 Executive summary

Dartmouth Secure Biometrics is a small start-up company about to launch its first product to the market. The company has developed a new, proprietary biometric technology that it plans to exploit for commercialization. The company has developed a product in the form of a bracelet that calculates a unique bio impedance signature. This signature can be used for personal identification. The company has completed all of its filings, applied for an application patent, completed systems testing on the bracelet and qualified a volume manufacturing facility. This marketing plan will detail how, when and where this company will not only launch this product but will also begin to generate revenue this fiscal year.

The health care industry is one of the fastest growing market segments in the US. With projections that spending will increase to 30% of the Gross National Product, this is a huge market and the company is positioned well to exploit it over the next several years. This document presents a detailed marketing plan on how it will enter this market this fiscal year (FY2013 07/2013-06/2014), and how it will reach exponential growth within the next 3 years. The company is currently managed by a small management team which possesses the skills critical to achieving this plan. Armed with proprietary technology, in the form of a biometric bracelet for personal patient identification in a hospital environment, Dartmouth Secure Biometrics has identified a specific target market to sell into.

The hospital emergency department and services have an increased need to accurately and efficiently identify the right patient through the entire system. The unique selling feature of this product is that it attaches to the patient and thus, provides a real-time wearable positive identification system that is currently not in place in hospital emergency department and services environment. Every minute counts for saving lives in an emergency setting.

In order to make this commercialization venture a success the management team is asking for $250,000 from investors and board members. In return the company will commit to delivering 3 signed contracts and $600,000 in revenue by EOFY 2013 that yields profits of over $400,000.

2 Overview

2.1 Company Overview - Dartmouth Secure Biometrics

Dartmouth Secure Biometrics was started to commercialize a biometric bracelet based upon bio impedance technology developed by Cory Cornelius at Dartmouth College. The bracelet is a new way to apply bio-impedance technology for personal identification. Currently, there is no way for electronic devices to automatically identify who is wearing an ID bracelet. Through his research, Cornelius was able to demonstrate that a bio impedance measurement through the wrist would create a unique signature because it used a combination of physical attributes including bone density, soft tissue and fluid. Specifically, it creates the signature by sending a small electric current to a bio impedance sensor and reads the opposition to the electrical current. The corporate logo shall start to be consistently used as shown in Figure 1 below.

Figure 1: Dartmouth Secure Biometrics Corporate Logo

The bracelet uses these readings to uniquely identify its wearer. The identification can then be securely transmitted or checked by other electronic devices in an unobtrusive manner. The device researchers from Dartmouth have come up with a new way to provide health monitoring through using a tiny electric current and a bio impedance sensor. Each person's body provides a different amount of opposition to electrical current, so bio impedance can be a unique biometric identifier. The researchers' idea is to create a bracelet that uses bio impedance readings to recognize its wearer in a secure, unobtrusive manner and communicate that identity to other wearable devices.

Using such a bracelet, "the devices discover each other's presence, recognize that they are on the same body (and transitively learn from the wrist device whose body), develop shared secrets from which to derive encryption keys, and establish reliable and secure communications." As opposed to other biometrics or password authentication, bio impedance readings can be taken passively, which is much more appealing than remembering pass codes or scanning fingerprints and retinas.

Researchers have created an eight-electrode bracelet, that takes a biometric measurement with a positive ID accuracy of 1 in 100,000 compiled a unique signature from blood, bone, and tissue impedance levels.

2.2 Introduction to Biometrics

Biometric technologies are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic. Biometrics are defined as the science and technology of measuring and statistically analyzing biological data [1]. Fingerprints, hand geometry, DNA, retina, iris, vein, and facial images are leading physiological biometrics. This type of measurement is unchanging and unalterable without significant duress. Behavioral characteristics are based on an action taken by a person and indirectly measure characteristics of the human body [2].

Biometric technology, like fingerprints starting cars or iris scans opening doors, were strictly relegated to science fiction at one time. It was a food for thought how soon this technology would turn from science fiction to real life and become an identification tool for everyday use. Due to the features like uniqueness, universality, permanence, measurability, and circumvention make this a popular technology gaining attention and acceptability in several fields [2]. Today all around the world, the governments, corporations, military establishments, and others are using biometric technology for identification across many different verticals for a multitude of objectives. There is biometric identification for workforce management to help stop time theft, build accountability, and reduce payroll error rates. Biometrics is used extensively in public safety to avoid duplicate booking entries, eliminate identity fraud, track inmate movements, and increase security. The financial industry has adopted biometric technology to reduce password expenses from fraud and protect customer data. Retail point-of-sale establishments use biometric identification to reduce false returns, helping improve loss-prevention strategies.

3 SWOT Analysis

The SWOT Analysis is performed to gain an understanding of and act on the product's capabilities and environment [1]. The product's capabilities, expressed as strengths and weaknesses, identify the product intrinsic characteristics with which the product can and cannot do well in the marketplace. The project environment, expressed as opportunities and threats, identifies the areas external to the organization in which the product will operate.

The SWOT factors were selected by the organization members based on literature review and past experience. These factors were then ranked using a Delphi method in a numeric scale from 0 to 3 as shown in Figure 2. The factors with the highest weights in the scale, highest chance or occurrence, were analyzed in depth and are described in the sections below.

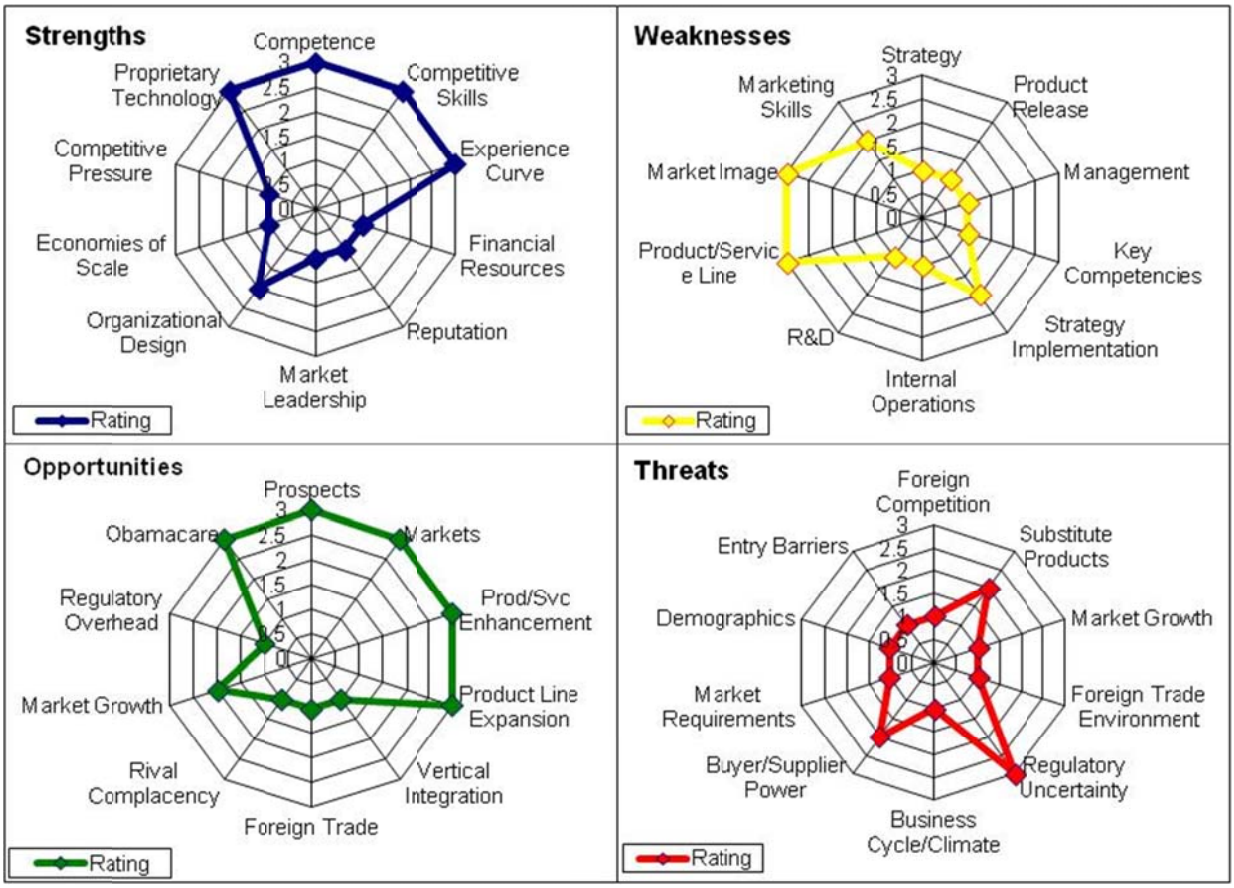

Figure 2: SWOT Analysis

3.1 Strengths

Competence

Our organization has a high level of competence in the technology development, new product development and commercialization. Our management team has experience and is familiar with the challenges in the health care industry.

Competitive Skills

We have competitive skills in the high technology market and the healthcare industry. However given the recent changes in the healthcare regulations our organization will have to re-learn many of the business practices required to succeed in the industry.

Experience Curve

Even though the product is still in development, our organization has experienced resources in New Product Development and Design for manufacturing that puts us ahead on the experience curve. Additionally because the bio-impedance technology is patented we will be able to further develop our mass production knowledge without any threats from other players in the industry.

Proprietary Technology

The bio-impedance proprietary technology is our major asset and the reason the company can be started with a solid business model that can be built around it. It is also a magnet for investors that see the market potential and are willing to fund the business while it ramps up production and revenue.

3.2 Weaknesses

We have identified two major Weaknesses our organization is faced with in the process of introducing the new product to the market

Market Image

Our product uses a new technology and has been developed in an academic center. Because of this the product has no commercial brand recognition and no history in the healthcare industry. Our organization will have to build the brand, company name, reputation, and, more importantly, the distribution channels in order to reach customers and users.

Product/Service Line

Our go-to-market is initially limited to a single product using the bio-impedance technology. Even when the product can be commercialized as a stand-alone device or as a part of a healthcare solution our organization recognizes this as a very narrow focus. Our management believes at this point this is the best use of the resources available to our start-up.

3.3 Opportunities

Markets & Prospects

Prospects refer to the additional customer groups that our organization could serve. For example, government agencies, high security facilities, the criminal justice system to name a few. These groups are further discussed in the market segmentation section.

Markets refer to the ability to integrate with healthcare solutions provided by other companies. We foresee that other companies with technology products will want to incorporate our solution into their systems because a) they will be in danger of becoming obsolete, b) the will be better able to track and monitor patients with the new e – systems being installed. For example, smart cards must partner with a biometric solution because they are "what the customer has". They need to deliver a higher security system to include "what the customer has + what they know + who they are". In this particular case our product will add the "who they are".

Obama care (Patient Protection and Affordable Care Act (PPACA))

According the U.S. Census Bureau, 48.6 million Americans lack health insurance, and millions more are under insured [3–5]. In 2011 the Patient Protection and Affordable Care Act (PPACA) was signed into law to extend coverage to roughly 50 million uninsured Americans, slowing down the growth in the cost of health care, and improving the quality of care in health care [7]. Local state and other federal guidelines provide the rest of the regulations [8]. All this is driving regulatory pressure for health providers to upgrade to e-record systems.

> ***"Legacy Systems and Business Processes:*** *Organizations using outdated processes and legacy technologies are struggling with significant backlogs and an inability to accurately pay claims in a timely fashion. Payers are facing increasing demand for more flexibility in plan design and higher levels of service while simultaneously lowering costs* [6]*".*

This is an opportunity for the health care industry as a whole, given that the most of the major provisions will be effective on January 2014 expanding the healthcare market by roughly 20%. [2]

Product/Service Enhancement

As a 'Product/Service Enhancement' this technology could be worn and integrated in several form factors. For example it could be worn as a wrist watch with the ability to identify the user and communicate with external systems via several wireless communication protocols. Additionally our organization could provide location services integrating GPS systems into a biometric device along with the ability for it to communicate real time pulse, blood pressure, and other real time measurements. A solar cell would be added to the surface of the device to allow for longer battery life at a slightly higher price.

Product Line Expansion

The bio-impedance technology could be implemented in accessories for portable devices so users can plug them in to their existing devices and utilize the same identification technology for a different range of applications.

3.4 Threats

Regulatory Uncertainty

While the Health Insurance Portability and Accountability Act (HIPAA) [9] and Patient Protection and Affordable Care Act (PPACA) government regulations have led to a higher rate of adoption of biometrics in healthcare applications, this also has created uncertainty regarding the required know-how to comply with these new regulations.

This has created a need for qualified healthcare and law professionals in the public and private sector that can successfully operate in the changing legal framework. This is a very important point to consider because it might have implications such as product release delays and product post-release legal issues.

Another intriguing aspect of the market is that many of the real and perceived threats represent significant opportunities for biometrics market development. For example, privacy and civil liberties advocates fear that widespread use of biometrics will enable a surveillance society. In this case biometrics could be the problem or the solution blurring the distinction between obstacle and opportunity. The most effective strategic response is to transform external threats into opportunities, making sure we comply with the legal framework and provide information to the consumer in an accurate and timely manner.

4 Market Analysis

4.1 Market Needs

The need to protect one's identity has become much more important. There are three established forms of identification in use:

1. Something you have (ID cards like passport or driver's license)
2. Something you know (Password or Pin)
3. Something you are (Signature, Iris, Voice etc. i.e. Biometrics) [10]

Current methods of human identification based on credentials (identification documents and PIN) are not able to meet the growing demands for stringent security in various industries such as security and border crossings, government benefits, medical etc. In the medical industry, proper patient identification is important to ensure that the right patient receives the right care. The Joint Commission [11], a private third party organization for assessing health care organizations, has classified the improvement of patient identification accuracy as the number one goal for last five years and also made this as a qualification requirement for hospitals. In addition, Obama Care has driven legislation to ensure patient rights [12].

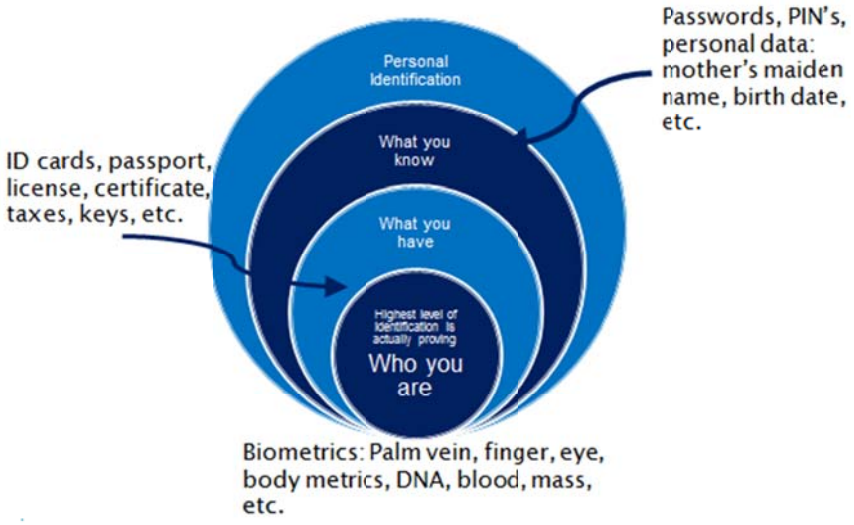

Figure 3: Increasing accuracy for the highest security requirements

Even within the highest, "who you are" biometric circle, as in Figure 3, there are different applications positioned to serve different markets. For example, biometrics such as signatures, voice and finger prints are excellent for securing assets such as cell phones, PDA's or laptops, but not considered to provide a high security required for door locks, server access, healthcare, or financial systems.

One industry is rapidly requiring security to the highest level in the form of positive personal identification. The healthcare industry is increasingly heating up to require a high level of positive patient identification. Checking the "Five Rights"—Right Patient, Right Medication, Right Dose, Right Time and Right Method of Administration—prevents most medication errors. However, often these five rights checks are faulty because they fail to guarantee the right patient [12]. There are three basic requirements that generate the need of identifying the patients with certainty which can be outlined as:

1. Reducing medical errors
2. Reducing risks of fraud
3. Improving capacity to react to medical emergencies

In the U.S., medical errors cause up to 98,000 deaths and 770,000 adverse effects annually, representing the eighth leading cause of morbidity in the United States, exceeding that of motor vehicles, breast cancer, or AIDS [13]. Approximately 1.5 million Americans are victims of medical identity theft. The healthcare fraud is estimated to cost between $70 billion and $255 billion per year, which accounts for between 3% and 10% of total U.S. healthcare costs [14].

Thus patient safety continues to be one of healthcare's most pressing challenges. There are many angles from which patient safety can be addressed. The prevention of duplicate medical records and the elimination of medical identity theft stand out as two of the main culprits jeopardizing the integrity of the healthcare industry. Incorrect patient identification

puts safety at risk and causes loss of money to the industry in administrative and legal expenses. These errors can be rectified and minimized using the adoption of biometric technology. Biometrics uses physiological characteristics of the human body for patient identification. Eliminating the need to provide an insurance card, social security number, or a date of birth for identification during registration & discharge, a biometric template can be directly linked to an electronic medical record for accurate credentialing on subsequent visits. This ensures creation of none duplicate medical records and also delivering of the right care to the right patient. Biometric patient identification helps to eliminate the sharing of medical insurance cards between patients. Further it also helps in identification of unconscious patients, those with the inability to speak, or who may have language barriers.

5 Product

Biometric Bracelets

The Body worn sensing devices are becoming a part of our day to day lives. These devices provide an easy way to measure physical activity (Fitbit bands, Nike Fuel, etc.), interact with entertainment devices (e.g., Nintendo Wii), or monitor their physiology (e.g., a cardiac patient concerned about heart arrhythmia or a diabetic managing her blood glucose). Despite of these advantages, in order to reliably interpret this data, there remains the challenge of recognizing, who is wearing that sensor. The family members in the same household might be using the same fitness measuring band or people might accidentally wear the wrong sensor, in either case there is no means for the device to authenticate the user unless there is a pin or a password associated with it. This becomes a crucial issue especially for the health care so as to correctly identify and store the correct health records. Thus there is a need of a device which people can use and does not required any action on the part of the user and can recognize whose body they are worn on [15].

Technology

The biometric bracelet uses the electrical characteristics of biological tissues in a person's body to recognize who is wearing the device. It measures the bio impedance – a measure of how the body opposes a tiny applied alternating current – at the person's wrist. Bio impedance is a physiological property related to a tissue's resistance to electrical current flow and its ability to store electrical charge. It is typically measured through metallic electrodes (transducers) placed on the skin and around an anatomic location of interest (e.g., the wrist). These electrical properties are predominantly a function of the underlying tissue being gauged, including the specific tissue types present (blood, adipose, muscle, bone, etc.), the anatomic configuration (i.e., bone or muscle orientation and quantity), and the state of the tissue (normal or osteoporotic bone, edematous vs. normally hydrated tissue, etc.). Significant impedance differences exist between the varying tissue types, anatomic configurations, and tissue state, each of which provides a unique mechanism for distinguishing between people. With this feature of uniqueness, each individual's identification will be single most effective identification for that user. This highly secured way of identifying users makes this technology less prone to

users to share access to highly sensitive data. The use of bio-impedance makes it extremely hard or impossible to duplicate or share biometrics accessing data with other users. Also, this specific user identification cannot be lost or forgotten which makes its use much easier than any other identification technologies [15]. The biometric bracelet allows real time information such as blood pressure, pulse, and other biological test to be provided to medical devices for fast and accurate diagnosis and treatment.

Form Factor

The device is a wrist band that contains small electrodes to measure bio impedance. This offers some technical advantages like the ability to wear it the same way every time it is used, which means that the issues with placement of the electrodes are diminished because it can sense data from nearly the same location each time and in the same orientation. Further, timer can be instrumented to detect when it has been placed on and taken off a person. Figure 4 shows the technology - product - system integration process with an early prototype design.

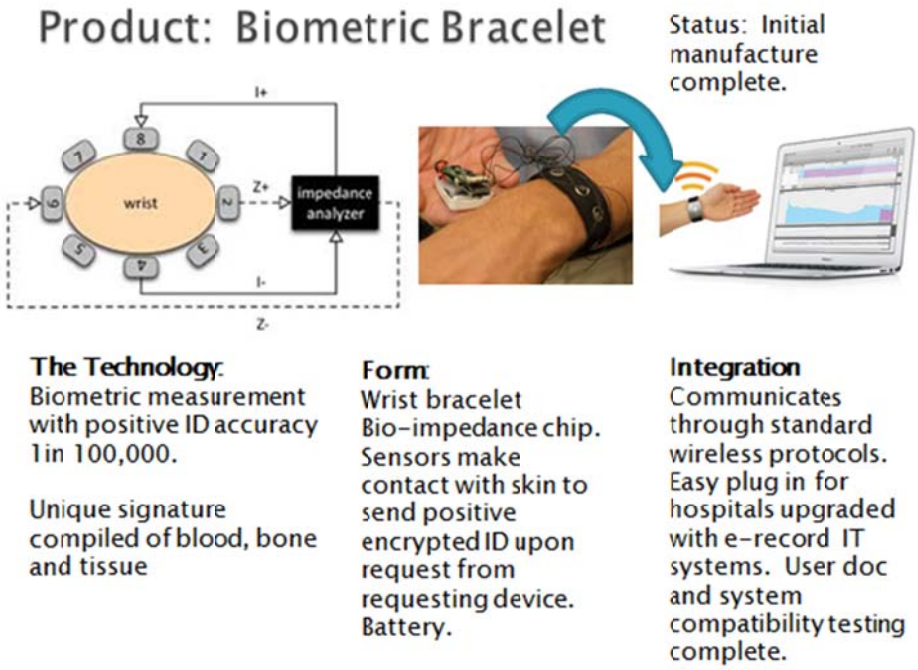

Figure 4: Biometric Bracelet Product

Biometric Bracelet Operation Life Cycle

The Biometric bracelet has a 7 step process that allows for the Identification, Access, Secure Communication, Real Time Data upload, and Encrypted closure of the medical files. This is shown in detailed in Figure 5 diagram below.

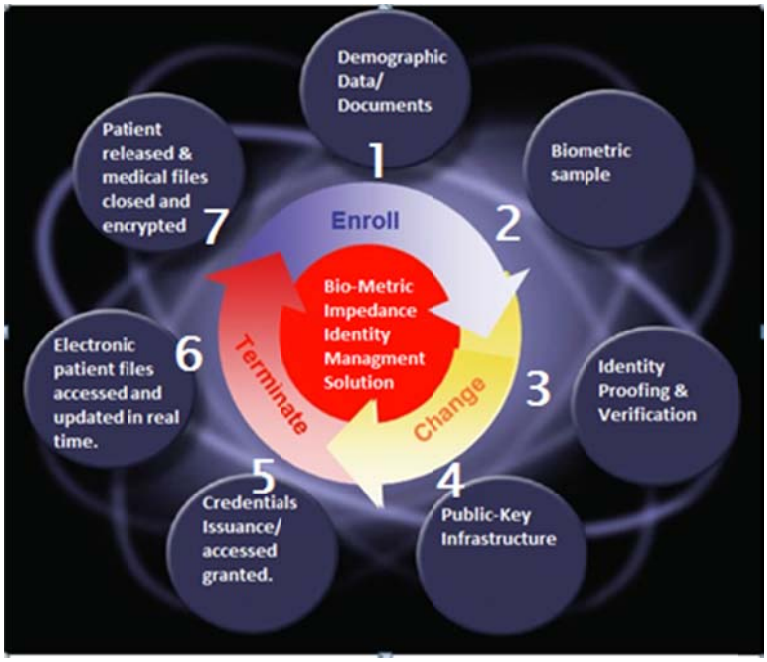

Figure 5: Biometric Bracelet Life Cycle

Step 1: The patient brings in documentation and demographic data to prove that the patient is who he/she says they are.

Step 2: The biometric sample is taken from the patient with the biometric bracelet providing a bio-impedance level of that patient.

Step 3: The patient's identity is proved and verification of the patient is finalized. This information is stored in the e-records system.

Step 4: After the identification of the patient is completed with a biometric impedance sample, the bracelet starts communicating with the hospitals internal wireless network using a public-key infrastructure to start secure encrypted communications.

Step 5: The bracelet provides credentials of the wearer to the medical instrumentation requesting access to the patient's secure files and to the functions of the medical instruments in the room.

Step 6: After the authentication process is completed the bracelet is given full access to send real time data and updates to the patient e-record files, via the medical instrumentation, which provide information to medical personnel in real time.

Step 7: At the end of the patience stay, the patient is released and the medical files are closed and secured. The bracelet is then removed and recycled, thrown away, or destroyed. If another person does get hold of the bracelet, the bio-impedance level will not match the previous wearer's levels and there for the files cannot be accessed.

Steps 4, 5 and 6 from this process describe in detail the interactions of the device with the IT infrastructure and the medical instrumentation. This is really the core of our competitive advantage, i.e. a device capable of providing real time authentication in the hospital room. This process is explained in further detail below.

Healthcare System Integration

The actual components of the IT Healthcare System that support the functioning of the bio-impedance bracelet are described as follows:

Hospital IT infrastructure: This is the network infrastructure that must be in place in order for the medical instrumentation to be able to communicate with a centralized e-records healthcare system. This is a broadband network backbone.

Medical Instrumentation: The medical instrumentation (e.g. IV dispenser, Medical Imaging device) is connected to the broadband network backbone via wireless and/wire line.

Bracelet: The bracelet communicates with the Medical Instrument via wireless either using a wireless antenna on the device or through the wireless IT infrastructure. The IT infrastructure wireless network has knowledge of the location of both the Medical Instrument and the Bracelet.

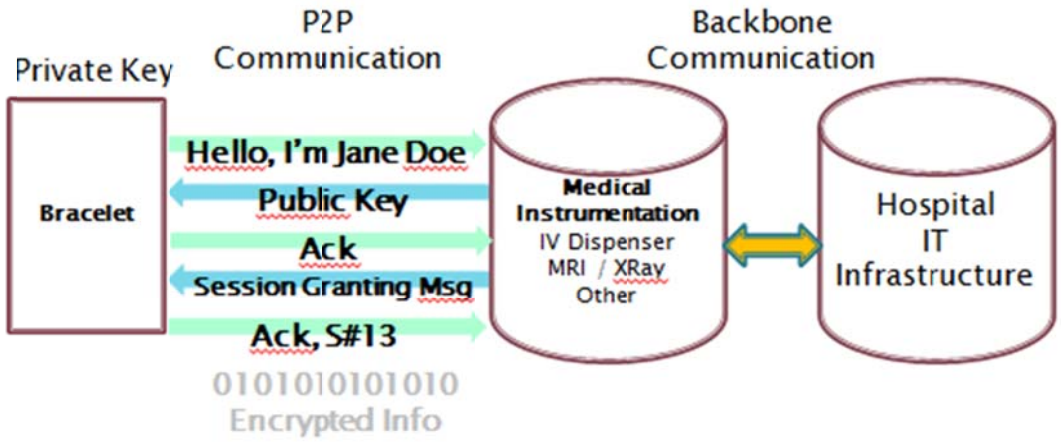

Figure 6 : Product operation in a hospital setting

The product communication process is designed to follow the steps below as demonstrated in Figure 6:

1. The Bracelet registers with the Medical Instrument by sending the wearer personal bio-impedance identification in an binary string encrypted with a private key

2. The Medical Instrument receives the binary string and decrypts it with a public key. It then searches the e-records systems in the E-Records Database, through the Hospital IT Infrastructure, to find the personal identification of the wearer.
3. Once the wearer has been identified, the Medical Instrument returns a message with a public key used to decipher messages
4. The bracelet receives the key and sends and acknowledge message to confirm the wearer identification
5. The instrument responds with a session id that confirms the bio-measurements taken will be recorded and identified as belonging to the wearer
6. The responds with acknowledgements and the session number at predefined customized time intervals to confirm the wearer is still present at the instrument. If the instruments stops receiving the acknowledgement it 'closes' the session

All recorded data is stored in the wearer's healthcare e-record system so the medical records are available on real time to the doctors, nurses and patient. This also allows for an accurate billing for the service care patients receive.

6 Target Market Selection

In order to find the right market segmentation, we considered the growth in global biometric technologies market and the global healthcare biometric markets. The US has the largest healthcare services market in the world. In 2010, the healthcare services industry accounted for approximately $1.75 trillion in revenues [16]. As of 2009, North America holds the second highest share in terms of total global biometric revenues which is about 37% [17]. Thus based on this data we chose the US healthcare biometric markets as our target market. In order to further focus on the right target market, the number of hospitals in US was considered. According to American Hospital Association [18], the total registered hospitals in US are 5724, of which over 40% have been upgraded with e-records. Out of that segment, 200 are equipped with the palm vein biometric technology at the registration desk as illustrated in Figure 7. [19], [20].

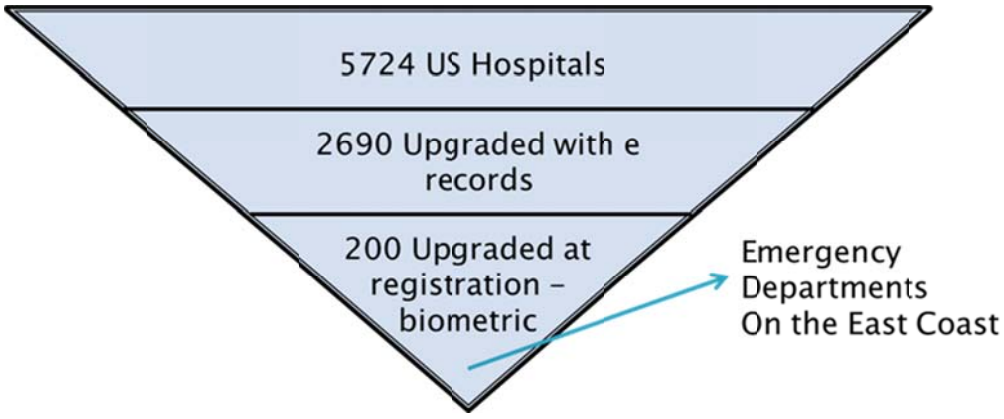

Figure 7: Market Segmentation

Currently, there are two main biometric technologies competing for the positive patient identification at the admissions desk: iris scan and palm vein. While the company has identified the hospitals that have been upgraded with the palm vein technology, the company knows through content analysis in a qualitative research study that a higher number of hospitals have the iris technology installed. The company estimates the number of hospitals with a highly secure identification technology to be around the 500 range, including the 200 with palm vein and those facilities with the iris scan technology.

In order to further refine the marketing segment, we focused on the number of hospitals with large emergency service departments. This segmentation is important because there would typically be a Director of Emergency Services who we would want in the room when we are performing our demonstration. These are the facilities that have partnerships with the life-flight and ambulance services. Then, our last segmentation is geographically related for cost savings as displayed in Figure 8. We are located in New Hampshire and will be targeting those facilities on the North Eastern part of the United States first.

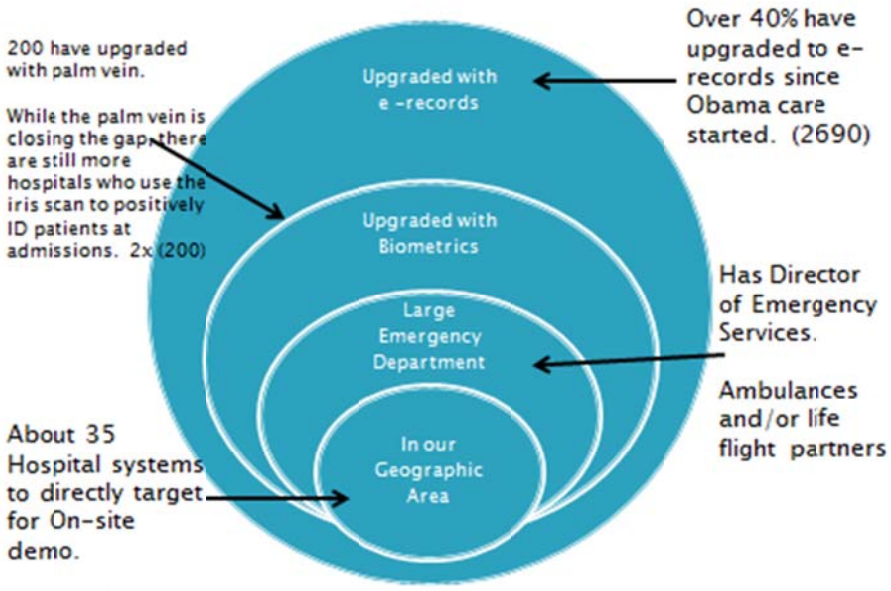

Figure 8: Refined Market Segmentation

7 Competition

There are several biometric technologies that are available and widely used for identification like finger scan, retina scan etc. As we can see from the Chart 1, below that the identity services is the most dominating application for the biometric industry. The Chart 2 shows the market share projection of these applications in identification until 2017. From this chart we can depict that the Automated Fingerprint Identification System (AFIS) and fingerprint scan enjoy the highest market share in the biometric identification.

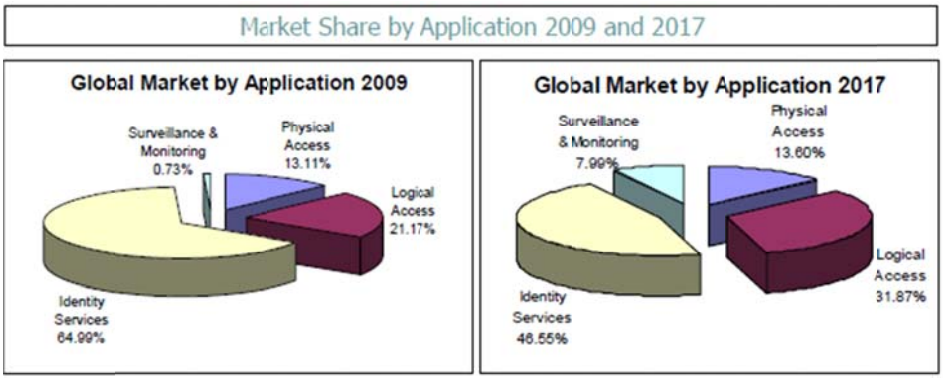

Figure 9: Source- Acuity Market Intelligence

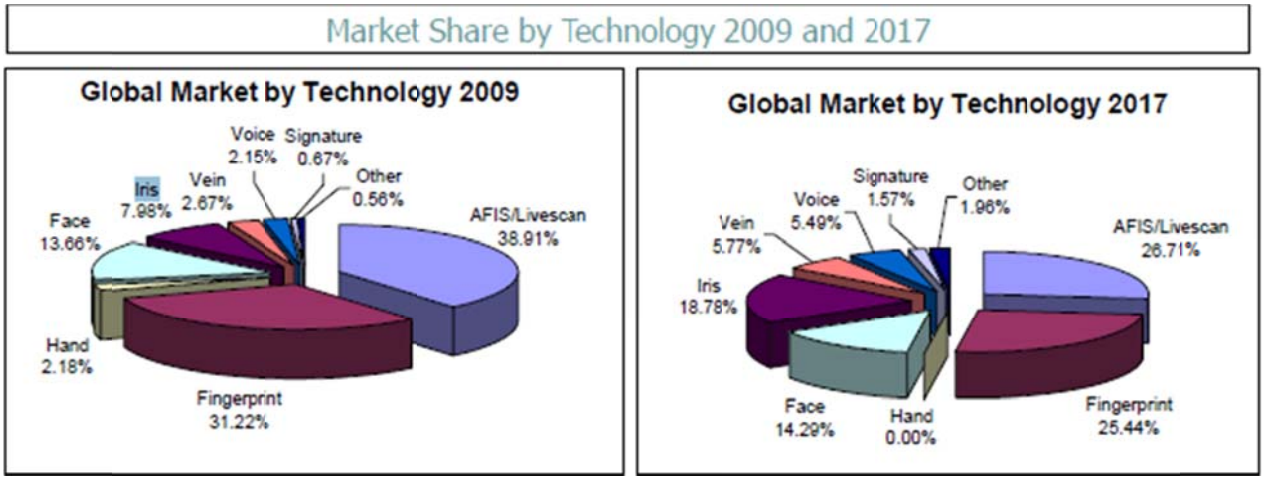

Figure 10: Source- Acuity market Intelligence

Further, the above listed technologies which use physiological characteristics can be compared on the seven factors [2] to assess the suitability of their use in personal identification.

Biometrics	Univer-sality	Unique-ness	Perma-nence	Measur-ability	Perfor-mance	Accept-ability	Circum-vention
Finger Scan	Medium	High	High	Medium	High	Medium	High
Facial Scan	High	Low	Medium	High	Low	High	Low
Retina Scan	High	High	Medium	Low	High	Low	High
Iris Scan	High	High	High	Medium	High	Low	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
DNA	High	High	High	Low	High	Low	Low
Signature	Low	Low	Low	High	Low	High	Low
Voice	Medium	Low	Low	Medium	Low	High	Low
Biometric Bracelet	High	High	High	High	High	Medium	Low

Table 1: Comparison of different biometric technologies:

From Table 1, we see that although the Fingerprint and AFIS are widely used, there are large tradeoffs for security and privacy when using these. Fingerprints can be changed or damaged and some people simply don't have fingerprints. Often because of these limitations fingerprint authentication systems have an alternative way of access through passwords which then become the weakest link in the authentication system. The other issue with finger print scanners that many manufacturers like Fujitsu, Shenzhen Yetong Technology Co. Ltd, Biosecurity Co., Ltd and others is that whenever a person goes somewhere they would have to use a figure print scanner to enter or exit a location in order to keep track of the patient. This is time consuming and can delay patient care.

The other technologies used currently in the market are the barcode identification and Radio-frequency identification (RFID). A barcode is an optical machine-readable representation of data relating to the object to which it is attached whereas RFID is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects.

The capabilities of barcodes and RFID pertaining to identification are identical. Barcode technology and RFID can help prevent medical errors by making accurate and reliable information readily available at the point-of-care. Wristbands with barcodes and RFID that contain the information of the patient's medical record or visit number, and any other identifiers have been proven effective to provide proper patient care [22].

Though Barcode technology is used widely, it has some disadvantages. Accuracy is a major drawback in barcode technology. Not every time is the barcode read accurately. A controlled check has to be performed to verify the accuracy of the barcode reading. Also, the reading distance of a barcode scanner is very short. Some readers need physical contact to the read the barcode symbols [23]. RFID systems are a better option to barcodes as far as the reliability is concerned. But RFID systems are expensive as compared to barcodes. RFID works best only when there is enough RF signal strength. This makes it less reliable as far as patient identification is concerned.

8 Positioning

In order to further analyze the technology and identify positioning points, a chart was compiled showing the companies technologies in terms of customer intrusiveness, cost and patient identification, PID, accuracy as seen in Figure 9. Improving accuracy is the driving factor to replace the current barcode bracelet. However, some of our target segments may be willing to trade on accuracy for cost or end customer (patient) acceptance. One factor measured to determine customer acceptance is how intrusive the technology is. For example, an iris scan is more intrusive than facial recognition because the patient may not be aware they are having their face captured by the camera. It may be totally non-invasive whereas a device close to the eye may be awkward and intimidating. The signature on the other hand requires a patient action but is scored as fairly non-intrusive because patients are typically conditioned to accept signing for transactions. The bio impedance technology may be worn as a wrist bracelet and

scored high as non-intrusive for similar reasons. While the device is worn, patients are typically accustomed to having wrist jewelry or watches. Dartmouth secure biometrics have made a note to use a user centered integration approach in our final product design to determine how much a "jewelry" look would factor in customer acceptance of our product. The chart based upon Fujitsu's palm vein scan market report was modified to fit our target market and competitors.

Only with a wearable bio impedance wrist device can health providers ensure that the right person gets the right medicine at the right time while reducing fraud and improving efficiency.

Our Positioning statement –

A wearable wrist device to provide secured real-time patient identification through the entire healthcare system.

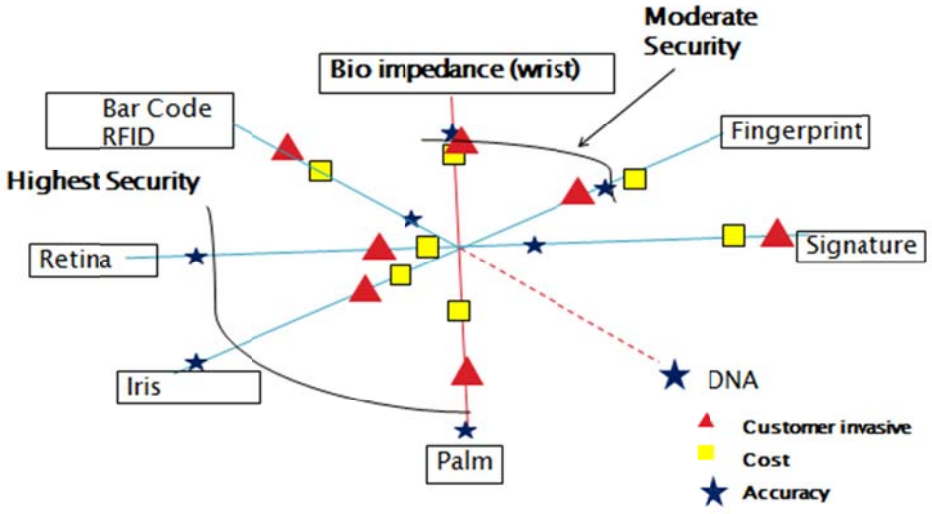

Figure 11: Comparison of different biometric technologies

9 Value Proposition

After understanding the target market segmentation, competition and the positioning of the product, the bio-impedance bracelet from Dartmouth Secure Biometrics offer three distinct value drivers that are listed below:

Safety – The "Five Rights" of a patient can now be extended into the rooms of the hospital past the admittance desk. It will provide additional safety for the patient that the right medication with right dosage at the right time using the right method of administration to the right patient is checked each time. Also it will be in line with the HIPAA security rule of protecting the privacy of individually identifiable health information.

Security – The bio-impedance bracelet will provide a fully integrated secure system in hospitals with increased data accuracy for patient identification thus reducing fraud and erroneous data. It will add on easily to systems in institutions that have upgraded e-record systems already in place. It will allow critical care patients the ability to go immediately through emergency admissions saving time while keeping the integrity of the patient identification secure.

Cost Saving – The bio-impedance bracelet will reduced the number of barcode readers which in turn will save cost for hospitals. Also it will eliminate the non-value added activities like scanning, reading barcodes, constantly securing patient identification in the hospitals.

10 CRTA: Compelling reason to Act

The 5 rights have been compelling many hospitals to upgrade their systems. Hospitals that have already made the decision to integrate positive identification with biometric technologies will be compelled to show a return on their investment. The biometric bracelet will allow hospitals to integrate this technology throughout the hospital environment with limited additional expenditure.

The Obama administration decided to tackle the problem presented by health providers resistant to integrating technology in their practices. In 2009, Obama signed the HITECH (Health Information Technology for Economic and Clinical Health) Act, which provides $27 billion in incentives for digital health record use [24]". This has all ready started to compel some providers to act. In 2009 only 46% [25] of US practices had incorporated electronic medical records. The Obama administration plans with the incentive to drive that number over 95%.

Second, fraud costs the health industry millions. Reducing medical identity fraud, which can leave hospitals with unpaid bills and consumers liable for care they didn't receive, is becoming more important. According to a survey, 50% of health-care organizations reported one or more incidents of medical identity theft. Furthermore, another study, performed by an organization that studies privacy, data protection, and security, reports that "data breaches at hospitals may cost the U.S. health-care industry as much as $7 billion a year [26]."

Several organizations have started integrating biometric technology at their admissions desks. The cost of $200 - $300 for an iris scan is now considered affordable; this is a cost that cannot be directly billed to the insurance company. The bio-impedance bracelet goes a step further by positively and securely identifying the person throughout their entire stay. The bracelet is not fixed to an entry point but is rather fastened to a person. While there are pros and cons to the other competing technologies, bio impedance can be measured unobtrusively and patients are already used to the bar code bracelet. For example, a microphone can capture a person's voice, a camera can observe a user's gait, or a malicious application could learn one's typing rhythm [27].

In contrast, recognition for wearable sensing applications demands a biometric that is simultaneously difficult to circumvent and easy to read on real-time. The biometric bracelet

with its unique bio-impedance feature, prototype testing on 46 respondents showed 90% accuracy in recognizing the correct wearer [15], and its low cost, relative to other biometric products, would serve as an attractive solution to hospital management and increase the precision on patient identification.

The bottom line is data breaches are costing U.S. hospitals over $7 billion a year and the U.S. government is offering incentives of $22 billion to integrate technology to protect patient rights. Health care providers are being financially compelled to act by both a stick and a carrot to the tune of almost $30 billion dollars.

11 Technology Adoption Life Cycle

The biometric bracelet is a breakthrough in the personal identification market. Thus this product will fall under the innovators phase when it is introduced in the market.

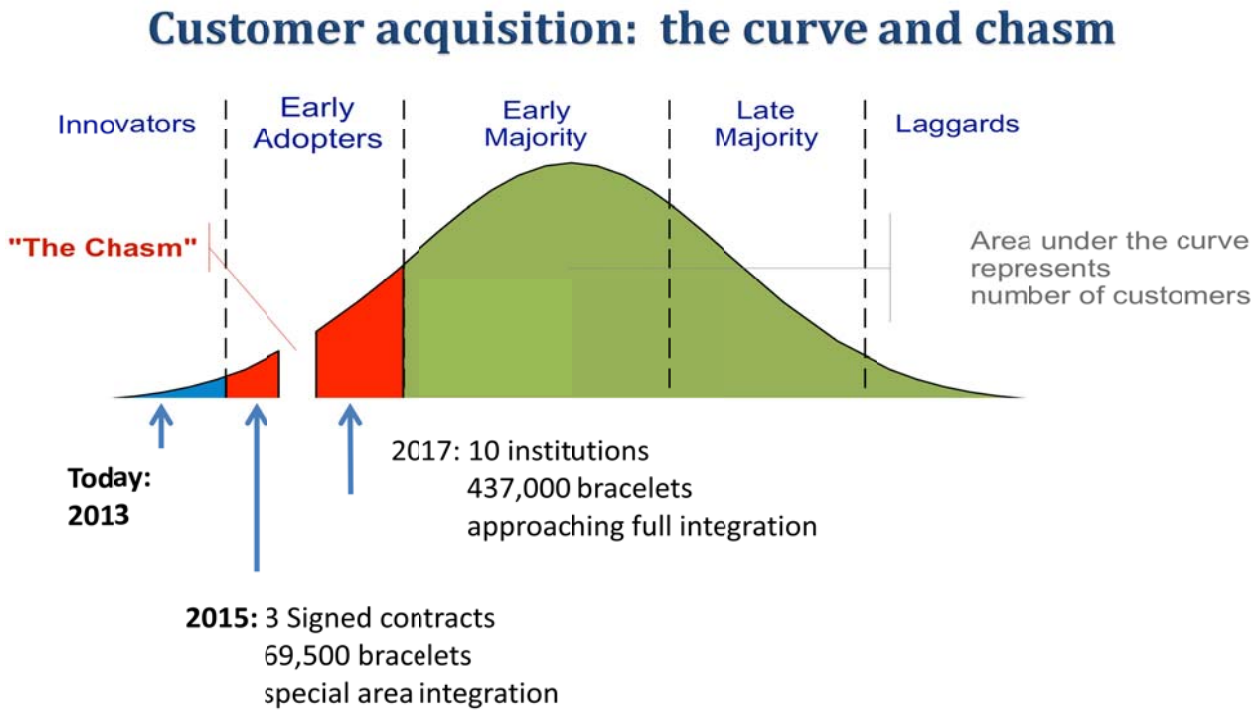

Figure 12: Technology Adoption Life Cycle

Per the adoption lifecycle shown in Figure 12, our product will be in the innovator stage at the time of launching. However, over the next fiscal year, we plan to capture the early adopter lifecycle gaining 3 contracts and selling about 7000 units to each hospital. The company's expects to cross "The Chasm" by EOFY2016 and sell close to 210,000 bracelets to 30 institutions. The sales forecast is further detailed on section 13 Budgeting and Control.

12 Marketing Mix

12.1 Place (Distribution)

While our volume is high, our actual customer base is small so it makes sense for the company to use a direct sales distribution model for the first 3 years. As mentioned in the Technology Adoption Life Cycle, during the 1st year the company will have a direct contract signed with the Director of Emergency Services with, at least, three institutions. These contracts shall be tightly managed directly by our Sales Manager. It is critical that we treat these customers as "Tier 1" so that we can establish a "beach head" and expand into other departments and hospitals within their system. This direct sales strategy will be deployed until we have reached 30 additional contracts.

The plan is as illustrated below in Figure 13:

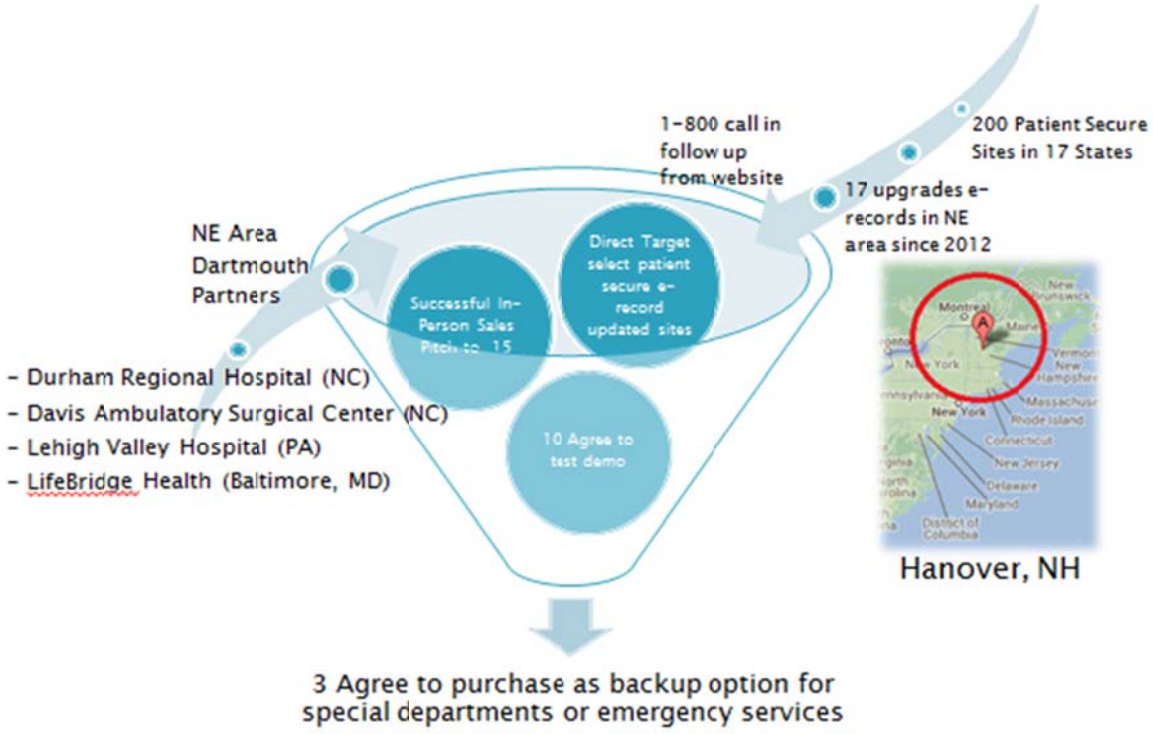

Figure 13: Beach Head Plan

Dartmouth Secure Biometrics will select patient secure e-record updated sites and starting in the NE around Dartmouth Secure Biometrics headquarters in Hanover, NH. Initial sites will potentially include the Durham Regional Hospital in North Carolina, Davis Ambulatory Surgical Center in North Carolina, Lehigh Valley Hospital in Pennsylvania, and LifeBridge Health in Baltimore Maryland to name a few. It is expected to get agreements to test our product as a demo in 10 of the potential customers and then to have 3 contract agreements to purchase our product for special departments or emergency services.

Biometric Partnerships:

Dartmouth secure biometrics is beginning to qualify a handful of value added resellers; VAR's to become our Biometric Partners. One reseller that specializes in biometrics is M2Sys [28]. This VAR meets the criteria of specializing in biometrics, represents multiple companies and has a pre-existing relationship with several of our targeted customers.

12.2 Promotion

Dartmouth Secure biometrics will start advertising on a small scale until resources increase. We will be using an *integrated marketing communication* strategy to create the awareness and promote the product to our customers.

In Figure 14, the pyramid outlines the promotional components that we will use for our campaign on the basis of reach and cost. This promotion will include various forms of traditional and online media. We will be using the catalogs and manuals to reach the mass target customer as a part of our awareness campaign. Also we will use print media for advertising in specialized magazines catered to health care products. Further participation in tradeshows and sending free product test samples along with the direct marketing will enable expansion of consumer knowledge of our biometric bracelet. Creating a dedicated webpage to introduce the product will encourage consumer interaction like feedback and queries. To provide an efficient customer service, we will set up a 24x7 toll free number.

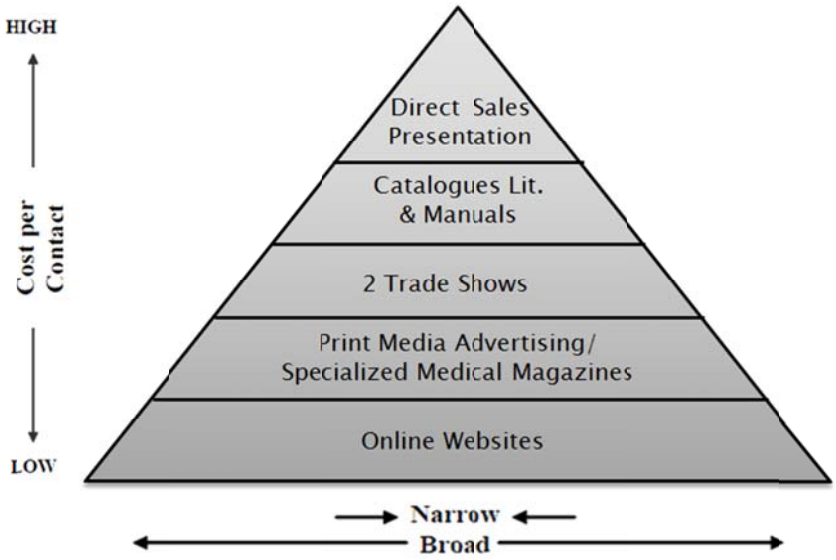

Figure 14: Promotion Strategies

For the introductory year, we estimated a total budget of $85,000 for promotion and advertising. We also budgeted $15,000 as contingency funds; should the need arise these can be added to the needed advertising media. The allocation of this promotional budget to these various tools for the year 2013 is shown in Table 2 below.

Method	Reach (Hospitals)	Objective	Cost	Detail
Direct Target Mkt site visit	15	Land a Sale, network, partner	$25,000	
Call/mail pkg cust.	100	Generate further interest. FAQ's	$5,000	
Trade Show	500	2 Shows, Live demo, network, extend call list	$15,000	All 3 attend: PI, Mkt, CIO
Print Ad	2,000	Customer awareness	$20,000	
Website	10,000	Inform, brand	$20,000	Create website, 1-800
Budget		3 site contracts	$85,000	
** Need $15,000 for contingencies				

Table 2: Budget for Promotion

12.3 Price (FY2013)

In order to calculate the pricing information for the newly introduced product three approaches were taken into consideration.

Manufacturing Cost

Table 3 shows the tier based manufacturing costs for the material. To determine the product's price we have used per unit cost of material. This can be extended further based on the quantity ordered. The pricing is computed for two different models – basic and advanced. As our bio-impedance bracelet resembles the form and basic concept of RFID Electronic Wristband with an additional bio-impedance property. We have used the costing of RFID Wristband as a reference point

Direct materials	
RFID Electronic Wristband*	US $0.07-0.68 / Piece
Static Bio metric chip cost	~US $0.25 - 1 / Piece
Static Bio metric chip cost	~US $0.10 - 1 Billion/ Pieces
Static Bio metric chip cost	~US $0.05 - 10 Billion/ Pieces
Programmable Bio metric chip cost	~US $3.00 - 1 / Piece
Direct Labor Costs	~US $1.00
Incremental revenue	~US $1.00 – Piece
Base Model	
Total for RFID Biometric ID Band*	Low end US $1.37
Total for RFID Biometric ID Band*	High end US $1.93

Advanced model	
Total for RFID Program able Biometric ID Band*	US $4.00

Table 3: Reference Manufacturing Cost (* Used as a reference)

Experience Curve

Dartmouth also estimated the volume based pricing. We estimate that the cost of manufacturing will decrease with the number of manufactured units. This is based on economies of scale and increased expertise of our OEM providers. Table 4 shows the ranges of volume and cost for manufacturing.

Volume Range	Cost
<10,000 units	$4.00
>10,000 and <=50,000 units	$3.00
>50,000 and <=100,000 units	$2.00
>100,000 units	$1.00

Table 4: Manufacturing Cost/Volume Relationship

In Figure 15 the relationships are illustrated for the Manufacturing Cost/Volume Relationship.

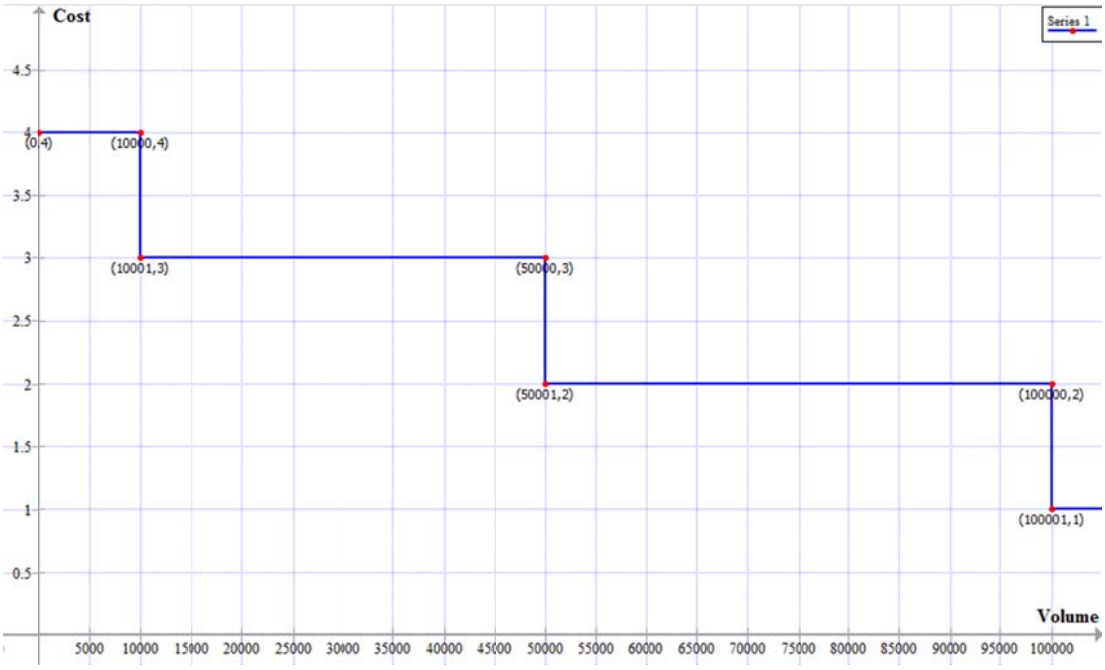

Figure 15: Manufacturing Cost/Volume Relationship

Value Pricing

Value pricing represents the customer perceived value of a product. This is the price the customer is willing to pay for a product given the benefit for the product final users. For example, a final user of the bracelet in the ER, where every second could be a matter of life or

death, would find more value than a user that is in interned in a hospital receiving treatment for a non-critical condition.

The bracelet value price composition is shown in detailed in Table 5. In addition to the customer perceived value the cost of the closest alternative (barcode) is added. This is because the barcode bracelet is considered a "supply" in healthcare accounting practices so it represents an expense for provider. On the other hand, a bio-impedance bracelet would be considered a "device" and is directly billable to the insurance company so the provider does not incur on any expense.

Replace bar code	$ Saved
Staff efficiency	$5.00
Scanner COW reduction	$2.00
Quality	$5.00
Cost of alternative (Barcode)*	$0.20
Total	$12.20

Table 5: Value Cost

The cost of the barcode alternative is calculated below as shown in Table 6; this includes the bracelet, label, scanner and printer required to operate the barcode scanning system [29] [30]. For this estimation a service unit with 10 scanners, 1 printer delivering 100,000 barcodes over its lifespan was considered.

Description / Product	Unit Cost * Number Of Units	Barcode Wristband/ Bracelet per piece
Wristband + Label	$0.19 * 100,000	$19000
Scanner	$49 to $ 99 Average $75 * 10	$750
Printers	$395 to $844 Average $ 449 * 1	$449
Total		$20199 ($0.20 per unit)

Table 6: Competition based model

12.4 Product

The product operation in a hospital setting is described in detail the 5 Product section.

13 Budgeting and Control

13.1 Financial Forecast

The total number of registered hospitals in US per the 2013 fast facts of US hospitals [18] is 5724. This data was used to compute the number of patients admitted per hospital which

was equalized to the requirement of the number of bracelets needed per hospital. Also, we estimated that every hospital will have a 10% buffer stock in addition to the requirement identified. According to the National Hospital Ambulatory Medical Care Survey 2010,the total emergency admissions in 129.8 million [21]. This averages out to be 22676 emergency admissions per hospital. The estimated number of Emergency Departments upgraded with IT systems that we could plug into is 400 from our target market research. Because our first phase targets the northeast our total targeted market opportunity is 19% of 400 times the number of emergency department visits.

Total Number of All U.S. Registered * Hospitals	5,724
# Hospitals in North East	1,088
# of Emergency visits per year **	129.8 million
# Emergency Admissions/hospital	22,676
# Emergency visits in North east per year**	24.3 million
# NE Hospitals in our target market (upgraded biometrics)	76
Total NE market opportunity – bracelets (current)	1.7 million
Bracelets needed for first 3 emergency department contracts	**69,000**

Table 7: Estimated Number of Bracelets per hospital ** Center for Disease Control website

Based on these estimations of customer demand, the revenue for the FYs 2013 to 2019 is projected as shown in Table 8.

Fiscal Year	FY2013	FY2014	FY2015	FY2016	FY2017	FY2018	FY2019
# New Emergency Dept Contracts	3	6	10	30	100	250	1000
# Existing Contracts	**0**	3	9	18	48	148	398
# Bracelets required (1,000)	69	207	437	1,104	3,404	9,154	32,154
Cost	$4	$3	$3	$1	$1	$1	$1
Price	$10	$10	$8	$7	$5	$5	$5
Revenue (1,000)	$690	$2,070	$3,496	$7,728	$17,020	$45,770	$160,770
Profit (1,000	$414	$1,449	$2,185	$6,624	$13,616	$36,616	$128,616

Table 8: Bio-Impedance Bracelet Sales forecast for FY2013-2019

The key to this forecast is signing the first 3 contracts. Once the first 3 contracts are signed, 3 more are forecasted to be signed the following year. In addition, we have not forecasted upswing of additional bracelet requirements as they are adopted into other parts of the hospital. We have strictly based this forecast on the emergency departments in those systems. As the demand will grow exponentially we will have to staff additional resources and look to our partnerships with qualified value added resellers.

The predicted sales forecast growth is better illustrated in Chart 4 showing the graph. One of the goals of developing this plan is communicating this forecast and the opportunity this business represents in order to secure grants, small business loans, and private funding from supporters to get the business up and running.

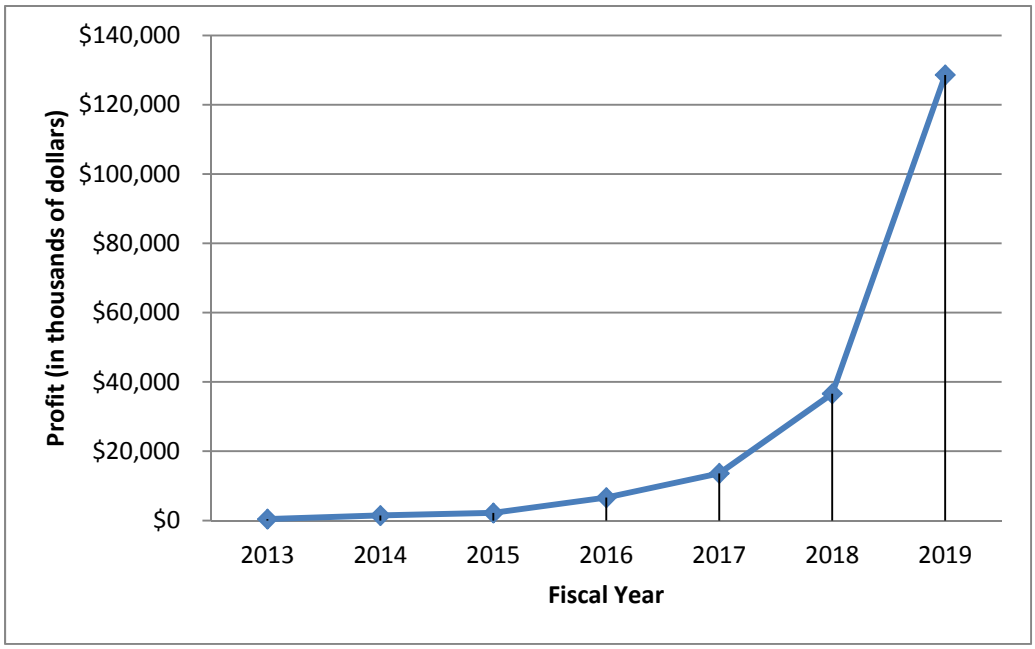

Figure 16 - Bio-impedance Bracelet Projected Growth

14 Conclusion

The highest priority for the management staff at Dartmouth Secure Biometrics is to sign 3 contracts this year. As soon as we have achieved this milestone, we will be primed and positioned to exploit our unique advantage. By aggressively selling into all emergency departments with healthcare e-record systems upgraded to handle biometric technologies we will expand our sales force to fulfill and service orders growing at an exponential rate. In reality, when we have reached the point of servicing 10 contracts we will have outgrown this plan. The environment of our company will have changed in order to face the challenges of exponential growth. We will be faced with additional challenges of defending our IP to extend our market advantage, supply chain problems, and the pressure to expand and improve our product line.

15 References

[1] K. P. Tripathi, “A Comparative Study of Biometric Technologies with Reference to Human Interface,” vol. 14, no. 5, pp. 10–15, 2011.

[2] A. K. Prabhakar, S. ; Pankanti, S. ; Jain, “Biometric Recognition: Security and Privacy Concerns,” *Security & Privacy, IEEE*, vol. 1, no. 2, pp. 33–42, 2003.

[3] D. I. Staff, “US Census Bureau Health Insurance main page.”

[4] “Uninsured Healthcare Tab- $49 Billion Annually.” [Online]. Available: http://insurance.about.com/od/reformresources/a/Uninsured-Healthcare-Tab-49-Billion-Annually.htm. [Accessed: 06-May-2013].

[5] “Most uninsured unable to pay hospital bills according to new HHS report.” [Online]. Available: http://insurance.about.com/gi/o.htm?zi=1/XJ&zTi=1&sdn=insurance&cdn=b2b&tm=48&gps=63_45_944_903&f=00&tt=2&bt=4&bts=4&zu=http://www.hhs.gov/news/press/2011pres/05/20110510a.html. [Accessed: 06-May-2013].

[6] Triple Tree, “HEALTHCARE REVENUE CYCLE MANAGEMENT A TripleTree Industry Analysis,” 2006.

[7] “The Affordable Care Act Turns Two | National Academy of Social Insurance.” [Online]. Available: http://www.nasi.org/discuss/2012/03/affordable-care-act-turns-two?gclid=CM_-xtjx-7YCFeeDQgodMHkATg. [Accessed: 06-May-2013].

[8] C. Systems, “International Profiles,” no. November, 2012.

[9] OCR, “Summary of the HIPAA Privacy Rule.”

[10] S. G. Davies, “How Biometric Technology Will Fuse Flesh and Machine,” *Information Technology & People*, vol. 7, no. 4, pp. 38–47, 1994.

[11] “Accreditation, Health Care, Certification | Joint Commission.” [Online]. Available: http://www.jointcommission.org/. [Accessed: 07-Jun-2013].

[12] Zebra Technologies, “It’s All in the Wrist: Improving Patient Safety with Bar Code Wristbands.” 2010.

[13] P. Duquenoy, C. George, and K. Kimppa, *Ethical, Legal, and Social Issues in Medical Informatics*. 2008, p. 320.

[14] “Why Healthcare should Evaluate Biometrics for Patient Identification | Porter Research.” [Online]. Available: http://www.porterresearch.com/Resource_Center/Blog_News/Blog/2012/September/Why_Healthcare_should_Evaluate_Biometrics_for_Patient_Identification. [Accessed: 06-May-2013].

[15] C. Cornelius, J. Sorber, R. Peterson, J. Skinner, R. Halter, and D. Kotz, “Who wears me ? Bioimpedance as a passive biometric.”

[16] “The Health and Medical Technology Industry in the United States | SelectUSA.” [Online]. Available: http://selectusa.commerce.gov/industry-snapshots/health-and-medical-technology-industry-united-states. [Accessed: 07-Jun-2013].

[17] M. Analysis, “The Future of Biometrics Market Analysis , Segmentation & Forecasts Insight into the Trends , Drivers & Opportunities that will Shape the Industry through 2020,” no. August, 2009.

[18] AHA Resource Center, “Fast Facts on US Hospitals.” 2013.

[19] C. Hall, “Texas Health hospital system uses palm scans to ID patients | Dallasnews.com - News for Dallas, Texas - The Dallas Morning News,” 2013.

[20] M. Anderson, “St. Peter’s Hospital implements hand-scanning technology | KXLH.com | Helena, Montana,” 2012. [Online]. Available: http://www.kxlh.com/news/st-peter-s-hospital-implements-hand-scanning-technology/. [Accessed: 07-Jun-2013].

[21] “National Hospital Ambulatory Medical Care Survey: 2010 Emergency Department Summary Tables.” .

[22] Niceware International, “Patient Safety with Bar Code and RFID Labeling Identification.” 2006.

[23] H. Kato, K. T. Tan, and D. Chai, “Barcodes for Mobile Devices,” *Cambridge University Press*.

[24] “American Recovery and Reinvestment Act of 2009,” *Wikipedia*. .

[25] “Medical Error | The Number Three Cause of Death in the United States.” [Online]. Available: http://www.therasim.com/industry-news/medical-error-deaths/#. [Accessed: 11-Jun-2013].

[26] K. Hallam, “Biometric Technology Combats Medical Identity Theft,” *Bloomberg Businessweek*, 2013.

[27] “Healthcare Biometrics Market - Global Industry Size, Share, Trends, Analysis And Forecasts, 2012 - 2018.” [Online]. Available: http://www.transparencymarketresearch.com/healthcare-biometrics-market.html. [Accessed: 06-May-2013].

[28] “Fingerprint Software SDK | Fingerprint Reader | Fingerprint Scanner.” [Online]. Available: http://www.m2sys.com/. [Accessed: 11-Jun-2013].

[29] “HC100 Wristband Printer.” [Online]. Available: http://www.zebra.com/us/en/products-services/printers/printer-type/desktop/hc100.html. [Accessed: 11-Jun-2013].

[30] “Zebra HC100 Wristband Label - The Barcode Experts. Low Prices, Always.” [Online]. Available: http://www.barcodesinc.com/zebra/hc100-labels.htm. [Accessed: 11-Jun-2013].

[31] "IBM Research: IBM 5 in 5: Biometric data will be the key to personal security." [Online]. Available: http://ibmresearchnews.blogspot.com/2011/12/ibm-5-in-5-biometric-data-will-be-key.html. [Accessed: 07-Jun-2013].

[32] R. Phaal, C. J. P. Farrukh, and D. R. Probert, "Technology roadmapping—A planning framework for evolution and revolution," *Technological Forecasting and Social Change*, vol. 71, no. 1–2, pp. 5–26, 2004.

[33] R. Phaal and G. Muller, "An architectural framework for roadmapping: Towards visual strategy," *Technological Forecasting & Social Change*, vol. 76, pp. 39–49, 2009.

16 Appendix A

- The ISO (International Standards Organization) and IEC (International Electro Technical Commission) put out a new standard to ensure security of personal and sensitive biometric data processed online.
- In February of 2011, Lumidigm and Imprivata partnered to deliver an integrated solution for healthcare clinicians to provide reliable and quick access to EMR applications even while wearing surgical gloves. Lumidigm also partnered with Verimetrics to deliver a leading biometric single sign-on solution for applications such as hospitals, emergency response vehicles, and retail stores.
- In July of 2011, SAFRAN finalized the acquisition of L-1 Identity Solutions, Inc.. This acquisition has strengthened SAFRAN's position in the biometrics market and in August , BIO-key International, Inc. Signed an agreement to acquire fingerprint manufacturer Montreal-based S.I.C. Biometrics Inc.
- In September of 2011, Nuance Communications, Inc. Closed the acquisition of Loquendo. This will help the company to offer a broad, and high-quality portfolio of solutions.
- Also in September of 2011, Biometric Signature ID, Inc. Entered into a partnership with Valtech to provide solutions that would greatly enhance the online security of its worldwide customers.
- Hospitals are switching to biometrics technology to enhance security, speed the admission process, and reduce avoidable errors.
- Some of the biometric technologies hospitals are using include fingerprint, palm readers, iris scanners, and voice recognition systems. These devices are used to identify a patient's medical record and track and control the sensitive information from being breached or tampered.
- The clinic Urban Health Plan in Bronx, New Year, has been using iris scanners for last two years to avoid mistaken identities and also to ensure that patient records are not mishandled.
- The Veterans Affairs Medical Center in West Palm Beach, Florida, has a voice recognition system to allow patients to access information over the phone.
- St. Vincent Hospital and Health Care Center, Inc., an Indiana-based healthcare provider will be deploying fingerprint biometrics scanners to enhance security and at the same time provide the speed and simplicity of access demanded by the users.

- Simply Healthcare Plans (SHP), a Florida-based HMO, will be implementing biometrics technology to curb fraudulent activities. The SHP customers will have their irises scanned at the initial point of contact at the healthcare facility [31].

Privacy law appendix

2007 – Personally identifiable Information. US Government memorandum. M-07-16
SUBJECT:Safeguarding Against and Responding to the Breach of Personally Identifiable Information
FROM: Clay Johnson III, Deputy Director for Management (2007/05/22)

2008 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)". NIST.

Some recent government initiatives driving the need to prove who you are through biometrics include:

Sec. 403© of the USA-Patriot Act which specifically requires the federal government to "develop and certify a technology standard that can be used to verify the identity of persons". This act has been used as a springboard for other Acts such as the Enhanced Border Security and Visa Entry Reform Act of 2002. In section 303(b)(1) of this act it reads that only "machine-readable, tamper-resistant visas and other travel and entry documents that use biometric identifiers" shall be issued to aliens. Currently the State Department is currently evaluating biometrics for use in U.S. border control pursuant to this act.

17 Appendix B – Product Development Roadmap

Technology Roadmaps provide a guide for technology and product development. The initial step in developing a Technology Roadmap is defining its nature. In our case we identified our technology introduction as a Technology Push, given that the technology at hand can be used to satisfy the needs of several different industries. The tools used to elicit the market drivers were largely based on previous studies in the TRM field [3].

Market Drivers

Based on the SWOT analysis, the Market Segmentation and the Customer Segmentation research the market drivers below were identified.

Market Drivers	Definition
D1 – User Identification	Refers to the ability to uniquely identify a user
D2 – Low Cost	Refers to a cost of acquisition and ownership below other products with the same features
D3 – Monitor Vital Signs	Refers to the ability to monitor and record/transmit patience vital signs

D4 – Connectivity	Refers to the ability to communicate with external devices and/or systems
D5 – Easy to use	Refers to the ease of use of the monitoring device
D6 – Non invasive	Refers to the ability to perform the monitoring functions without needing to force an entry in the patient
D7 – Location	Refers to the ability to provide the device location

Table 1: Market driver definitions

Product Features

The primary function of our initial product is the ability to uniquely identify users using a bio-impedance chip. As it was done in the previous section, all of our product features were identified.

Product Features	Definition
P1 – User Identification	Refers to the ability to uniquely identify a user
P2 – Battery Powered	Product operates on long lasting batteries
P3 – Networking	Products can have network connectivity which enables it to retrieve information remotely.
P4 – Medical monitoring	The product can have add-ons to monitor user vital signs
P5 – Location	Refers to the ability to provide location services using GPS and/or Wireless Network

Table 2: Product Feature Definitions

Technologies

In this section, we tried to come up with technological capabilities that supported the product features identified in the section above. The technological capabilities are shown in the table below.

Technological Capabilities	Definition
T1 – Bio-impedance	Bio-impedance is explained in further detail in the Technology (add cross-reference) section.
T2 – Wireless Communication Protocols	Common off the shelf protocols like Bluetooth and NFC (An Amulet for Trustworthy Wearable mHealth) and custom secure communication protocols specifically built for healthcare applications (*Plug-n-Trust: Practical Trusted Sensing for mHealth*).
T3 – Battery Technology	Battery technology plays an important role in the initial product due the fact that it could be a potential limitation of our product compared to other identification technologies.

T4 – Location Services	GPS and Wi-Fi technologies allow tracking the device location and would open the door to whole new set of location services.
T5 – Vital Signs Monitoring	Sensing technology to monitor heartbeat rate, blood pressure, glucose levels and other vital signs.

Table 3: Technological Capability Definitions

Resources

Initially the organization technology resources will be limited to in-house R&D. Once the products are moved the manufacturing phase the company will rely on the OEMs and suppliers from the Electronics Manufacturing Industry supply chain.

Resources	Definition
R1 - In-house R&D	This refers to the company's internal R&D capabilities
R2 - Semiconductor industry	The semiconductor industry would be one of the most critical sources for medical technology. Also, new designs will likely provide more energy efficient devices and consume less power.
R3 - Networking Technologies	The networking technologies allow interconnectivity in the medical infrastructure.
R4 – Healthcare Software Industry	Organizations Implementing advanced communication as well as potential monitoring and diagnostic applications. The firmware used for basic device handshake communications is out of the scope of this Resource.
R5 – Healthcare Electronics R&D	Refers to the R&D resources from other organizations in the industry
R6 – Location Services Vendors	Refers to organization providing location and mapping services, e.g. Google Maps, Bing Maps, which can be integrated in a custom location solution

Table 4: Resources Definitions

Results

Using the TRM analysis techniques of Phaal [32], [33], the four levels of the TRM were analyzed. The results of this analysis were then run through Brainstorming and the Delphi Method in order to elicit the industries our technology could be applied to. This yielded a set of Technology Considerations the company can use to target selected industries with a variety of products.

The Technology Considerations include external factors, such as the nature of technological change and competitor activity, and internal factors such as technological capabilities. Three key factors were used to stimulate the development of the product roadmap [32]:

- Basis: The selection of a generic strategic approach (e.g., cost leadership, differentiation or focus)

- Direction: Identification and Selection of alternative directions (e.g., do nothing, product development, market development, consolidation, market penetration, integration, diversification)
- How: The identification and selection of alternative methods (e.g., internal development, joint development, acquisition).

In order to identify market drivers the company explored the personal identification market through literature review and experts consultation. The outcomes of this process are the selected industries shown in the table below; the table also shows the particular sector and use scenario within the industry.

Personal Identification	National Security	User Monitoring
Biometrics	**Biometrics**	**Biometrics**
U1. Healthcare Identifier **(Beach Head)** U2. Corporate Security	U3. DoD U4. Government	U5. Healthcare Monitor U6. Sports U7. Family Care

Table 5: Dartmouth Secure Biometrics Potential Industries & Sectors

U1. Healthcare Identifier (Beach Head): This Use Case is covered by our beachhead product which addresses the need for user identification in the healthcare industry.

U2. Corporate Security: A corporate facility grants levels of physical access to users uniquely identified by their personal impedance. Additionally the device could be used to provide logical access to computer systems

U3. DoD: In the military a machine (e.g. aircraft, tank, weapon) could require the user to identify himself in order to allow its operation. This could also help track boots on the ground location and their vital signs.

U4. Government: Government secure facilities would require employees/visitors to identify themselves at all times via a wireless monitoring system providing different access levels depending on the product user. This could be implemented in Intelligence Agencies, DoJ Agencies and National Laboratories.

U5. Healthcare Monitor: A next generation Bioimpedance bracelet monitors patient vital signs and records them or transmits them to an external system. The device is integrated with full healthcare solutions provided by other vendors, e.g. GE, Siemens, Fujitsu; based on secure communication standards.

U6. Sports: A bracelet is used to monitor vital signs and location of sportsmen. In addition it sets a fashion trend with a functional accessory.

U7. Family Care: A bracelet is used to monitor vital signs of infants, children, and people with disabilities.

To create the roadmap, the company verified the connections between the market drivers, product features, technology capabilities and the resources based on the findings from the literature research. It then established the time line for the future product timelines, these potential products would attempt to address the Use Scenarios listed above. The product released dates are decided on the basis of technology, market drivers and our organization's ability to succeed in the marketplace with the previous product releases.

Timeline	2013-2015	2015-2017			2017-2023		
PRODUCTS	**U1. Healthcare Identifier**	**U2. Corporate Security**	**U5. Healthcare Monitor**	**U7. Family Care**	**U3. DoD**	**U4. Govt.**	**U6. Sports**
MARKET DRIVERS D1. User Identification D2. Low Cost D3. Monitor Vital Signs D4. Connectivity D5. Easy To Use D6. Non invasive	**D1, D2, D4, D5, D6**	**D1, D4, D5, D6**	**D1, D3, D4, D5, D6**	**D1, D2, D3, D4, D5, D6**	**D1, D3, D4, D5, D6, D7**	**D1, D4, D5, D6**	**D1, D3, D4, D5, D6, D7**
FEATURES P1. User Identification P2. Battery Powered P3. Networking P4. Med. Monitoring P5. Location	**P1, P2, P3**	**P1, P2, P3**	**P1, P2, P3, P4**	**P1, P2, P3, P4**	**P1, P2, P3, P4, P5**	**P1, P2, P3**	**P1, P2, P3, P4, P5**
TECHNOLOGIES T1. Bio-impedance T2. Wireless Comm. T3. Battery Tech. T4. Location Services T5. Vital Signs Monitor.	**T1, T2, T3**	**T1, T2, T3**	**T1, T2, T3, T5**	**T1, T2, T3, T5**	**T1, T2, T3, T4, T5**	**T1, T2, T3**	**T1, T2, T3, T4, T5**
RESOURCES R1. In-house R&D R2. Semiconductor Ind. R3. Networking Tech. R4. Healthcare Sw. Ind. R5. HC Electronics R&D R6. Location Svc. Vend.	**R1, R2, R3**	**R1, R2, R3**	**R1, R2, R3, R4, R5**	**R1, R2, R3, R4, R5**	**R1, R2, R3, R4, R5, R6**	**R1, R2, R3**	**R1, R2, R3, R4, R5, R6**

Table 6: Dartmouth Secure Biometrics Products Timeline

The TRM building process gives emphasis to the business strategy, sustainability and growth. All while increasing out competitive advantages and reducing our technology and business expertise gaps.