BIOMETRICS – IMPLEMENTING INTO THE HEALTHCARE INDUSTRY INCREASES THE SECURITY FOR THE DOCTORS, NURSES, AND PATIENTS

By: Darrell Shawl

THESIS FOR MASTERS DEGREE
INFORMATION ASSURANCE
CAPS795
DAVENPORT UNIVERSITY
PRESENTED TO:
DR. LONNIE DECKER

November 10, 2013
Abstract

Mistakes are made in our healthcare systems more and more these days. You hear about records being mixed up, medical charts are confused among patients; the wrong medication is given to the wrong patient. Healthcare biometrics refers to biometric applications in doctors’ offices, hospitals, or for use in monitoring patients. This can include access control, identification, workforce management or patient record storage. Biometrics has revolutionized the healthcare industry; devices can take unique information about you from your eye, your hand print, or your thumb print and use it to identify you. This information can be used to ensure that you are who you say you are, and you have permission to be working with the healthcare information you are trying to access.
Table of Contents

Abstract...........................................................................................................................................2

Table of Contents.............................................................................................................................3

Introduction.........................................................................................................................................5

Literature Review................................................................................................................................6-7

Purpose...........................................................................................................................................7

  Need for Biometrics in Healthcare.................................................................7-8

  Multispectral Biometrics.........................................................................................8-9

  Biometric Identity in Healthcare...........................................................................9-10

  Fingerprint Biometrics..........................................................................................10-11

  Biometrics Increase Security and Improve Efficiency.....................................11-12

  Biometric Technologies......................................................................................12-14

  Selecting a Biometric Technology.................................................................14

  Comparison of Biometric Technology..........................................................15

  Impact on Security and Policy........................................................................16-17

  Benefits of Combining Smart Cards and Biometrics...................................17-19

  Importance of a Quality Image.........................................................................19-21
Introduction

With the healthcare industry looking to implement electronic health records, there is rampant optimism about how digitizing health records will create massive efficiencies and significantly increase the quality of patient care. As more and more hospitals and healthcare systems migrate to computerized physician order entry and electronic health records, and more health information exchanges are built to coordinate care across networks, many are raising concerns about how to effectively manage data integrity to ensure it is kept free from corruption, modification, or unauthorized access.

The proliferation of healthcare electronic health records (EHRs) and the transition of data across health information exchanges (HIEs) open the door to data corruption, and as these systems become larger and more complex, vulnerabilities grow. In most other industries, data integrity is just as important, but corruption errors can be rectified and mistakes fixed. This can mean the difference between life and death within the healthcare industry.

One of the primary concerns with maintaining data integrity is implementing a consistent approach across the health information exchange to matching patients with their data. Both physicians and patients have to trust and rely that data is complete, current, accurate, and secure. Escalating the complexity of health information exchange as more networks are added and more data is fed into the system will only necessitate a concentrated effort by the entire industry to produce common standards that foster confidence data stays intact. The ultimate solution to maintaining end-to-end data integrity doesn’t originate from one company but must be a collective and cost-effective effort from all healthcare providers across the industry.
Health information exchange data integrity and quality care originates with accurate patient identification. There is simply no other step in patient care that is more important within the modern healthcare construct than precise patient identification to ensure that not only is the right care delivered to the right patient, but that medical records are up to date, accurate and properly linked across systems.

**Literature Review**

Since biometric deployments in healthcare have traditionally been extremely difficult and problematic, this paper will be focusing on implementing it into the healthcare industry and trying to support this hypothesis statement.

Hypothesis: By implementing biometrics it can increase the security for doctors, nurses, and patients. How does the healthcare industry use a biometric system? What kind of issues are there within the healthcare industry by using biometrics? What was done to fix those issues? What kinds of benefits have been gained from using biometrics? After working in the computer field for the past 15 years and having several friends that work in the healthcare industry; implementing biometrics in healthcare is critical to help reduce the risk of patients getting incorrect medication or results.

Most conventional biometric systems fail to operate reliably in the harsh environments and situations found in most hospitals today. Frequent hand washing, heavy use of chemicals and cleaners, the wearing of latex gloves and a wide range of demographic issues make biometric enrollment and authentication quite difficult and challenging. Because dry skin is so prevalent in the healthcare industry due in part to constant hand washing, traditional fingerprint sensors can produce up to a 20 percent failure rate.
Healthcare workers wearing latex gloves do not want to remove them to use the biometric reader. However, multispectral fingerprint sensors capture fingerprint data beneath the surface of the skin so that dryness or gloves create no problems for reliable reads. That is why biometric implementations using multispectral fingerprint sensors are becoming the solution for hospitals that spend $100 to $200 per employee per year supporting password based systems and even more for token or card based systems while trying to ensure the protection and safety of patient information.

**Purpose**

The purpose of this paper is to explain how implementing biometrics into the healthcare industry will address identified security issues and increase information security for doctors, nurses, and patients. How does biometrics play a role in security within the healthcare industry to help protect not just the doctors and nurses but also the patients?

**Need for Biometrics in Healthcare**

The need for biometrics in the healthcare industry is growing at astronomical rates; the worldwide market potential is currently estimated at $1.9 billion. A significant driver in biometric market growth rates is the HIPAA Act; HIPAA imposes stringent new federal requirements to protect patient privacy and the confidentiality of patient information. This is causing all healthcare facilities to begin developing compliance procedures for meeting these new standards. As a result, healthcare institutions are beginning to embrace the deployment of biometrics. Institutionalizing biometrics does indeed compliment the strategy in assuring HIPAA compliance through (Schneider, 2001):

- User authentication
Biometrics also creates operational efficiencies for all ID procedures, it provides improvements to risk management programs by ensuring that accurate patient identification is tied into care or treatment plans or matched to medical records management systems for each individual patient. It also offers for the first time what many agencies have wanted – the concept of a universal patient identification number that provides positive identification of an individual using a biometric tied to a unique number. And lastly, the overall quality of care is improved through accurate patient and/or staff identification.

Multispectral Biometrics

Multispectral biometrics plays an important role in healthcare applications, especially when there is a need to control access through positive identification of authorized users. HIPAA regulations mandate patient confidentiality and biometrics can help ensure that only authorized personnel gain access to those records. Biometrics help minimize insurance fraud and theft of controlled inventories such as pharmaceuticals and they can secure against the unauthorized use of expensive medical equipment (Spence, 2011).

In addition to controlling access, multispectral biometrics plays a role in facilitating operational efficiency in healthcare. Most security solutions are designed to block rather than facilitate transactions. However, carefully designed biometric systems can streamline operations
by providing quick and easy access to authorized users. Biometric systems can enforce and document compliance with hospital policies and procedures, enhancing patient and staff security.

Biometrics is only viable if the technology and solution can be made to work reliably for every user, every time. The cutting edge biometric technology multispectral fingerprint which has the unique ability to see beneath the surface layer of skin is having a dramatic impact on user performance and real world experience in the healthcare industry. Not only can multispectral fingerprint handle the environmental factors that can affect fingerprints, but it is also the only technology on the market today that can extract a fingerprint image from a gloved hand (Spence, 2011).

**Biometric Identity in Healthcare**

Biometric technology represents the future for positive healthcare identification and will enhance the secure use, storage, and exchange of personal health information. The lack of patient identity safeguards present many issues for patients and providers, patients are victims of medical identity theft so that their records may contain health data and claims that are not theirs, jeopardizing treatments in the future and health care financial limits. Patients may have their medical records falsified to support fraudulent claims when they have not received care. Fraudsters can use providers and patients identities to falsify claims, all of these issues lead to less safe and efficient patient care.

State and federal budgets face increasing pressure to reduce or contain spending without reducing services. The prevention of healthcare fraud allows more dollars to be available for necessary healthcare services. The use of biometrics to secure patient and provider identities can prevent certain healthcare fraud, thus increasing the efficiency and effectiveness of healthcare
programs. Biometric identity solutions deter and reduce fraud by (Biometric identity in healthcare: Reduces health care fraud, improves patient care and protects patient privacy, 2011):

- Preventing card sharing and patient identity theft by authenticating the patient in the provider’s location.
- In fee-for-service programs, preventing provider billing for “phantom claims” or services when a patient is not at the provider location on the service date.
- Verifying managed care “encounter data” or services from providers so that Medicare and Medicaid programs can rely on this reported data for setting of managed care rates.
- Creating an “audit trail” of check in and check out times for comparison against type of service provided as an indicator of potential fraud called “upcoding.”

**Fingerprint Biometrics**

As more healthcare networks begin storing patient records electronically, they have become increasingly concerned with security and many are turning to biometrics. For instance a healthcare provider in Arizona recently introduced fingerprint biometrics at its facilities to help secure patient records and increase efficiency. Arizona’s Children’s Clinics for Rehabilitative Services installed DigitalPersona Pro’s data protection and access software as well as U.are.U fingerprint readers to prevent unauthorized personnel from accessing patient records. These new systems are helping to protect the clinic’s more than 11,700 patient records which have been stored digitally in its electronic health record system. The new fingerprint biometrics has not only improved security but also expedited patient care and minimized the need for IT personnel
to help recover lost or forgotten passwords, it also enabled to simplify and speed up the login process.

Before Arizona’s Children’s Clinics implemented biometric technology they were relying on using usernames and passwords to access clinic resources. Roughly 40 percent of the clinic’s staff consists of part-time contractors who only deal with patients a few times a month and as a result many forgot their passwords resulting in lengthy delays for providers and patients. Using the fingerprint readers has enabled providers to quickly access electronic health records (EHRs), patient rooms are now equipped with a computer where doctors can electronically access patient’s data and with the new USB fingerprint readers doctors can log in with a quick touch of their finger. Fingerprint biometrics reduces the chances that patient records can be viewed by the wrong person by preventing the sharing of authentication credentials. It also helps healthcare organizations be more efficient since they don’t have to deal with people losing or forgetting their fingers (Fingerprint biometrics help secure medical data at Arizona hospitals, 2011).

**Biometrics Increase Security and Improve Efficiency**

To improve privacy and security measures, Saratoga Hospital in New York partnered with DigitalPersona Inc. to install biometric access controls to verify medical personnel’s identities and increase efficiency. Due to awkward username and password authentication process, hospital officials have difficulty accurately tracking access to its sensitive data networks. Passwords can be cumbersome and oftentimes personnel would stay logged in to avoid having to manually type a password each time they needed to access patient information thus, making it difficult to track who had accessed information. In addition, when an individual logged into a computer it would lock the system down, forcing the next user to reboot the system to gain
access. With fingerprint readers, employees can now login with a simple swipe of a finger and it also expedites the processing of documents by allowing users to sign electronically with their fingerprints. By having fingerprint readers on computers that can be wheeled into hospital rooms it allows the nurses to move throughout the day to do their various duties without having to type their individual username and password in multiple times (Saratoga Hospitals Deploy Biometrics to Increase Security and Improve Efficiency, 2012).

**Biometric Technologies**

Biometric technologies are defined as automated methods of identifying or verifying the identity of a living person based on unique biological (anatomical or physiological) or behavioral characteristics. Biometrics can provide very secure and convenient verification or identification of an individual since they cannot be stolen or forgotten and are very difficult to forge. Four major components are usually present in a biometric system (Smart Cards and Biometrics in Healthcare Identity Applications, 2012):

- A mechanism to scan and capture a digital representation of a living person’s biometric characteristic.
- Software to process the raw biometric data into a format that can be used for storing and matching.
- Matching software to compare a previously stored biometric template with a template from a live biometric sample.
- An interface with the application system to communicate the match result.

Two different stages are involved in the biometric system process – enrollment and matching. During the enrollment stage the biometric sample of the individual is captured using a
sensor for fingerprint, microphone for speech recognition, camera for face recognition, camera for iris recognition. The unique features are then extracted from the biometric sample to create the user’s biometric template. This biometric template is stored in a database or on a machine readable ID card for later use during a matching process.

![Figure 1. Example Enrollment Process](image)

**Figure 1. Example Enrollment Process** (Smart Cards and Biometrics in Healthcare Identity Applications, 2012)

During the Matching stage the biometric sample is again captured, these unique features are extracted from the biometric sample to create the user’s live biometric template. This new template is then compared with the templates previously stored and a numeric matching score is generated based on a determination of the common elements between the two templates. System designers determine the threshold value for this verification score based upon the security and convenience requirements of the system.
Figure 2. Example Matching Process (Smart Cards and Biometrics in Healthcare Identity Applications, 2012)

Selecting a Biometric Technology

The selection of the appropriate biometric technology will depend on a number of application-specific factors, including the environment in which the identification or verification process is carried out, the user profile, requirements for matching accuracy and throughput, the overall system cost and capabilities, and cultural issues that could affect user acceptance. High, medium, and low are denoted by H, M, and L. Values assigned for how each biometric identifier meets the various qualities are subjective judgments, based on expert opinion (Smart Cards and Biometrics in Healthcare Identity Applications, 2012).
<table>
<thead>
<tr>
<th>Biometric Identifier</th>
<th>Maturity</th>
<th>Accuracy</th>
<th>Uniqueness</th>
<th>Failure-to-Enroll Rate</th>
<th>Record Size</th>
<th>Universality</th>
<th>Durability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>84-2,000</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L-M</td>
<td>250-1,000</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Hand</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>9</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Iris</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>688</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Signature</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>500-1,000</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Vascular</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>512</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Voice</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>1,500-3,000</td>
<td>H</td>
<td>L</td>
</tr>
</tbody>
</table>

**Table 1. Comparison of Biometric Technologies** (Smart Cards and Biometrics in Healthcare Identity Applications, 2012)
A key factor in the selection of the appropriate biometric technology is its accuracy. When the live biometric template is compared to the stored biometric template in a verification application, a similarity score is used to confirm or deny the identity of the user. System designers set the threshold for this numeric score to accommodate the desired level of matching performance for the system, as measured by the False Acceptance Rate (FAR) and False Rejection Rate (FRR). Biometric system administrators will tune sensitivity to FAR and FRR to get to the desired level of matching performance supporting the system security requirements.

- The False Acceptance Rate indicates the likelihood that a biometric system will incorrectly verify an individual or accept an imposter.
- The False Rejection Rate indicates the likelihood that a biometric system will reject the correct person.

**Impact on Security and Policy**

The key social issue surrounding biometrics is the seemingly irrevocable link between biometric traits and a persistent information record about a person. Unlike most other forms of recognition, biometric techniques are firmly tied to an individual's physical traits. The tight link between personal records and biometrics can have both positive and negative consequences for individuals and for society at large. Convenience, improved security, and fraud reduction are some of the benefits often associated with the use of biometrics.

In order to achieve these benefits for a biometrics based authentication method, the particular biometric traits must be stored remotely in order to be available to multiple systems. Remote storage raises concerns about what security measures are in place to protect the biometric information, what personnel have access to the stored information, and how the
individual’s privacy and civil liberties are protected. In order for multiple systems to have access to the database for authenticating individuals’ identities, both an open application interface and tightly controlled and monitored access control mechanisms are required. However, as a system becomes more widely available, there is greater risk of a system or personnel security breach. Data breaches are a significant and growing problem for the healthcare industry (Smart Cards and Biometrics in Healthcare Identity Applications, 2012).

Biometrics systems have the potential to collect and aggregate large amounts of information about individuals. Almost no popular discussion of biometric technologies and systems take place without reference to privacy concerns, surveillance potential, and concerns about large databases of personal information being put to unknown uses. Privacy issues arise in a cultural context and have implications for individuals and society even apart from those that arise in legal and regulatory contexts. The problems arising from aggregating information records about individuals in various information systems and the potential for linking those records through a common identifier go well beyond biometrics and the challenges raised have been addressed extensively elsewhere.

**Benefits of Combining Smart Cards and Biometrics**

When implementing biometrics in an identity application, combining the biometrics implementation with a smart card brings a number of benefits. Using smart card technology significantly enhances privacy in biometric ID systems. Smart cards can store and match the biometric on the card, enhancing user privacy. When a biometric match is requested, the biometric reader submits a new live template to the smart card; the smart card then performs the matching operation within its secure processor and securely communicates the result to the
identification system. This method protects the initial enrolled biometric since it is maintained within the smart card and never transmitted off the card, the cardholder privacy is also maintained with this technique since the cardholder’s biometric template information is not readable from the smart card. An ID system using the combination of smart card technology, cryptographic functions and biometrics has significant security advantages, including (Smart Cards and Biometrics in Healthcare Identity Applications, 2012):

- Using digital signatures to ensure that the biometric template being used has not been altered.
- Using encryption to protect the biometric template and other personal information stored on the smart card.
- Using the smart card to compare the live biometric template with the biometric template stored on the card. Since the biometric template never leaves the card, this protects the information from being accessed during transmission and helps to address users’ privacy concerns.
- Using a cryptographic challenge to authenticate the legitimacy of the card and the reader. This ensures a very high level of privacy for the cardholder, prevents inappropriate disclosure of sensitive data, and helps to thwart skimming of data that might be used for identity theft.

Healthcare organizations considering different approaches for verifying patient and healthcare provider identity must look at the privacy, security, usability and performance implications of the different options. Smart health ID cards – either alone or combined with biometrics provide a privacy sensitive, secure solution, and also offer additional features and functions that can provide significant benefits to healthcare providers when compared to a
biometrics only solution. Biometrics only solutions are not ideal for patient health ID cards, a smart health ID card with a photo provides a solution that patients are familiar with and will readily accept. The smart health ID card also promotes the healthcare organization brand, can support a wide variety of applications that add value, and can be interoperable and usable among disparate groups.

Combining smart cards and biometrics can provide a full feature solution for healthcare provider identity authentication. By storing the biometric and performing the biometric match on the smart ID card, the privacy and security of biometric authentication are enhanced and system performance is improved with local offline identity authentication. Smart card technology is used globally for secure identity, access and payment applications. As a standard based technology, smart card solutions for patient and provider identity management are deployed around the world and are available from numerous vendors. Smart card technology provides a strong foundation for health ID cards enabling improvement in healthcare processes and in patient and provider identity verification while securing information and protecting privacy (Smart Cards and Biometrics in Healthcare Identity Applications, 2012).

**Importance of a Quality Image**

In order for biometrics to provide positive outcomes, the accuracy or quality of finger imaging is paramount. If images captured are not reliable, the risk of error due to improper or inaccurate identification increases dramatically. The technology hurdle that had to be overcome was improvement in the data acquisition portion of traditional, optical based fingerprint systems and processes, which typically would take about 20 minutes to capture a set of fingerprint
images. In the healthcare industry, biometric fingerprint imaging requires the highest level of accuracy, which eliminates user error as well as boasts technological accuracies.

The principle on which optical fingerprint scanners operate is well known and based on the difference in the indices of refraction of skin, air and the fingerprint platen to obtain a live-scan fingerprint image. Because of the limited depth of penetration, this technology is particularly sensitive to the surface conditions of the skin. Thus, performance of optical systems is inherently less than satisfactory. Limited depth of penetration of light waves results in imperfect imaging of the fingerprint (Schneider, 2001).

![Ridge Structure of a Finger](image)

**Figure 3. Optical Imaging Theory of Operation** (Schneider, 2001).

The properties of ultrasound permit imaging beyond air gaps and surface contamination into the true ridge structure of the fingerprint. Because ultrasound penetrates many materials the scanner is not sensitive to the surface contaminants typically found on the finger and platen, making it the clearly superior technology. The characteristics of sound waves are the ability to penetrate materials, producing an echo at each interface.
Figure 4. Ultrasonic Imaging Theory of Operation (Schneider, 2001).

Advantages of ultrasound include:

- Ultrasound has the ability to penetrate many materials, sending back echoes at each interface.
- Consequently it passes through contamination on the finger or platen, imaging the true ridge structure.
- Images are compatible with existing databases.
- Higher quality fingerprint images produce greater accuracy in ID matching.
  - All populations are covered
  - Contaminants on the finger and platen are transparent
  - Enables successful unattended applications
  - Images can even be captures with the use on certain latex gloves
• Optical scanning encounter problems with: dry fingers, oily fingers, contaminated fingers, irregular ridge structures, very low humidity and with contaminated platens.

In addition, independent laboratory testing has demonstrated superior accuracy results of ultrasound versus optical scanning. The graph compares data on 4,014 fingerprint images from 259 people. The results are clear: ultrasound is as much as 10 times more accurate in routine use, the test demonstrates that with no false acceptances, optical systems gave a false rejection rate of 12%, compared to the ultrasonic rate of 1% (Schneider, 2001).

Table 2. Fingerprint Images Graph (Schneider, 2001).

Research Methodology

When Arizona’s Children’s Clinics for Rehabilitative Services installed data protection and fingerprint readers to prevent unauthorized personnel from accessing patient records it showed how much it was helping to protect the clinic’s more than 11,700 patient records which
have been stored digitally in its electronic health record system. The new fingerprint biometrics has not only improved security but also expedited patient care and minimized the need for IT personnel to help recover lost or forgotten passwords as well as simplify and speed up the login process (Fingerprint biometrics help secure medical data at Arizona hospitals, 2011).

A new report focusing on the healthcare biometrics market predicts that the sector was valued at 1.2 billion dollars in 2012 and is expected to grow 25.9% from 2013 to 2019, to reach an estimated value of 5.8 billion dollars in 2019. Rapid technological advancements in healthcare infrastructure, increasing accuracy and performance levels, along with reduced complexity and cost of biometric devices are some of the major factors driving the biometrics growth in healthcare. The global healthcare biometrics market can be categorized into biometric technologies and their applications in various authentication processes. Fingerprint recognition technology is the most prominently used biometric technology and it is predicted that it will make up more than 50% of biometrics demand in healthcare industry through 2019.

Meanwhile, hand, vein, face, and iris recognition are expected to witness fastest growth. Demand for these products will benefit from more strict government regulations and industry standards covering the safety, security, and functional features of biometric systems. Logical access control is essential for user’s authentication to permit access to computer systems in hospitals and healthcare facilities. The logical access control segment is expected to dominate the global healthcare biometrics market during the given forecast period of 2013 to 2019.

Geographically, North America is expected to remain the largest market for healthcare biometrics technologies. Currently, North America along with Europe captures more than 75% of the market share. In the developing world, Asia-Pacific region will provide the largest and
most diverse sales opportunities for biometrics security solutions in the healthcare sector due to budding domestic and export markets for nationally produced biometric devices (A Strong Pulse for Biometrics in Healthcare, 2013).

Checking with the Network Specialist at Fayette Regional Healthcare System in Connersville, Indiana which is the local hospital in the town that I live in to see if they use any type of biometrics within their facility and found out that with them being a small town hospital that they did not use any biometrics for their security and he doesn’t see any being implemented in the future due to financial reasons and they have just implemented a barcode system for distributing medicine to their patients. The patient wears a bracelet that has a barcode on it that is scanned by the nurse which in turns scans the barcode on the medicine to confirm that they match. The only type of biometrics that the hospital uses is an electronic ID card that the employees use to clock in and out for their shift, when they clock in it displays the employee’s information. They also use radio frequency identification (RFID) which is used to access certain areas within the hospital, when they enter one of these areas it logs their employee ID and grants them access if authorized.

**Recommendations**

As biometric patient identification systems continue to evolve, one can expect to see more multifactor authentication solutions that combine multiple modalities for patient identification such as iris and facial recognition. This provides healthcare with additional tools to accurately identify patients in the event of injury or trauma. Some recommendations of using biometrics within healthcare include:
• Implement mobile biometric patient identification throughout a hospital to confirm the identity of patients at various touch points such as pre-op, medication dispensing and outpatient services.

• Increase ability to communicate with identifying an unconscious patient or those with the inability to speak or who may suffer from a language barrier.

• Increase data integrity standards across health information exchanges (HIEs).

• Implement biometric automated systems to decrease the potential for inaccurate patient identification.

• Implement Voice Authentication – The client’s voice is their password, there is no need to remember passwords, PINs, policy numbers or other challenge info.

• Implement Voice Signature – Secure, legally binding signature over the phone using client’s voice print.

Summary

Biometrics is the use of automated methods to recognize a person based on a physiological or behavioral characteristic. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Several examples of biometric technologies include fingerprint, face, retinal, and iris recognition as well as hand geometry. The use of biometrics is rapidly becoming the de-facto means of person authentication in healthcare because there is no other method more safe, secure, affordable, or efficient. In the healthcare industry, biometrics is replacing costly, inefficient, and jeopardous ID card PIN, or password systems, and the facilities embracing it are realizing immediate benefits (Healthcare Biometric Identity Management Technology):
• Employee and patient identity is established with irrefutable proof and correctness  
• Healthcare professionals are held more accountable for their actions  
• Significant realized cost savings in the administration and reproduction of ID cards or PINs  
• Ease-of-use saves time that can be redirected to improve patient care  
• People can never forget or share their fingerprints  

Only identity verification solutions based on smart card technology can provide identity assurance and authentication while increasing privacy and security. Smart cards also bring operational efficiencies to the healthcare system that reduce costs, reduce fraud, and increase patient satisfaction. As electronic health records (EHRs) and personal health records (PHRs) move to the mainstream, smart health ID cards can be used as a two-factor authentication mechanism into a provider or insurer web portal. Smart health ID cards protect patient privacy and security when accessing online records and support the National Strategy for Trusted Identities in Cyberspace (NSTIC) which identifies consumer access to online electronic health records as warranting two-factor authentication.
Conclusion

All over the world, 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 inflation and 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 and protect customer data. Retail point-of-sale establishments use biometric identification to reduce false returns, helping improve loss prevention strategies.

Patient safety continues to be one of healthcare’s most pressing challenges, although 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. Costing the industry millions of dollars per year in administrative costs, legal expenses and liabilities, in addition to placing patient safety at risk, the root cause of these problems are generally inaccurate patient identification, a problem that can be rectified through 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. A biometric template can be directly linked to an electronic medical record for accurate credentialing on subsequent visits. This ensures that no duplicate medical records can be created and the right care is delivered to the right patient. Biometrics also eliminates difficulties in identifying patients with the same name or multiple surnames helping to
ensure that each time a patient visits a healthcare facility, their medical history is properly documented no matter what variation of their name is provided (Trader, 2012).
References


http://www.planetbiometrics.com/article-details/i/1745/


http://www.ibia.org/download/datasets/727/

Fingerprint Biometrics Help Secure Medical Data at Arizona Hospitals. (2011, August 30). Retrieved September 15, 2013, from


http://www.ultra-scan.com/Portals/16/PositiveOutcomes.pdf


http://www.securityinfowatch.com/article/10473265/hospitals-can-finally-put-a-finger-on-biometrics


## Appendix A – Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EHR</td>
<td>Electronic Health Records</td>
</tr>
<tr>
<td>FAR</td>
<td>False Acceptance Rate</td>
</tr>
<tr>
<td>FRR</td>
<td>False Rejection Rate</td>
</tr>
<tr>
<td>HIEs</td>
<td>Health Information Exchanges</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>NSTIC</td>
<td>National Strategy for Trusted Identities in Cyberspace</td>
</tr>
<tr>
<td>PHR</td>
<td>Personal Health Records</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
</tbody>
</table>
Appendix B – Tables and Figures

Figure 1. Example Enrollment Process (Smart Cards and Biometrics in Healthcare Identity Applications, 2012)

Figure 2. Example Matching Process (Smart Cards and Biometrics in Healthcare Identity Applications, 2012)
<table>
<thead>
<tr>
<th>Biometric Identifier</th>
<th>Maturity</th>
<th>Accuracy</th>
<th>Uniqueness</th>
<th>Failure-to-Enroll Rate</th>
<th>Record Size</th>
<th>Universality</th>
<th>Durability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>84-2,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L-M</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>250-1,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hand</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iris</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>688</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>500-1,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vascular</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1,500-3,000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 1. Comparison of Biometric Technologies* (Smart Cards and Biometrics in Healthcare Identity Applications, 2012)
Figure 3. Optical Imaging Theory of Operation (Schneider, 2001).

Figure 4. Ultrasonic Imaging Theory of Operation (Schneider, 2001).
Table 2. Fingerprint Images Graph (Schneider, 2001).