The Review: A Journal of Undergraduate Student Research

Volume 15 Article 4

2014

Health Care Information Technology: Securing the Electronic Health Record with Biometric Technology

Alyssa Iacona
St. John Fisher College, aiacona_no@sjfc.edu

Health Care Information Technology: Securing the Electronic Health Record with Biometric Technology

Abstract

The principal focus of this paper is to examine the integration of biometric technology into healthcare's information technology systems. Biometric technology, a rapidly evolving mechanism, analyzes specific anatomical and physiological features of an individual for identity verification (Perrin, 2002). Moreover, as the federal government has mandated all health records to be electronic in 2014, the implementation of biometrics has become a prevalent means of security. In an effort to adhere to the patient privacy laws authorized by the Health Insurance Portability and Accountability Act (HIPAA), biometric recognition is currently used to restrict access to verified health care providers and detect fraudulent account access. This paper considers the advantages, disadvantages, and ethical consequences of utilizing biometric technology to secure the electronic health record in regards to cost, usability, accessibility, and accuracy. In addition to evaluating the primary application, the essay acknowledges the potential use of biometric technology to identify patients by vasculature scanning in the future.

Health Care Information Technology: Securing the Electronic Health Record with Biometric Technology

Alyssa Iacona

Abstract

The principal focus of this paper is to examine the integration of biometric technology into healthcare's information technology systems. Biometric technology, a rapidly evolving mechanism, analyzes specific anatomical and physiological features of an individual for identity verification (Perrin, 2002). Moreover, as the federal government has mandated all health records to be electronic in 2014, the implementation of biometrics has become a prevalent means of security. In an effort to adhere to the patient privacy laws authorized by the Health Insurance Portability and Accountability Act (HIPAA), biometric recognition is currently used to restrict access to verified health care providers and detect fraudulent account access. This paper considers the advantages, disadvantages, and ethical consequences of utilizing biometric technology to secure the electronic health record in regards to cost, usability, accessibility, and accuracy. In addition to evaluating the primary application, the essay acknowledges the potential use of biometric technology to identify patients by vasculature scanning in the future.

Introduction

Over the past few years, the privacy and security of health records has been an issue of increasing concern. Innovation to health record information protection is largely facilitated by use of technological advancements, which is especially needed in coordination with the elevated prevalence of electronic health records. For instance, the use of biometric technology is currently on the rise as a means to protect and secure the electronic health record (EHR). As with use of any technological advancement, implementation of biometrics in healthcare has many advantages as well as disadvantages. In conjunction with the drawbacks of biometrics, sociocultural, ethical, and legal consequences may arise. Although the disadvantages of biometrics may be consequential, the benefits should be acknowledged and considered for future use of privacy and security of electronic health records.

Description of Biometrics

To begin, an explanation of biometrics allows for better understanding of how the technology is currently utilized in the health care world. Biometric technology is a type of recognition system which identifies an individual by analyzing anatomical and physiological characteristics (Perrin, 2002). An individual's fingerprint, face, iris, hand geometry, palm print, odor, voice, and signature are a few examples of characteristics used for scanning and identification (Zuniga, Win, & Susilo, 2010). Biometric technology enrolls a person into a system by scanning and extracting the traits of the individual's characteristic, which is then stored as a template in the system's database. With each following scan, the characteristic of the individual will evoke the system to extract specific traits and generate a match to the person's unique template, enabling access to the system (Jain, 2007).

History of Biometrics

Although the technology used for biometrics seems rather new, the identification method has been traced back thousands of years. The use of biometrics

dates back to 500 B.C. in Babylonia, when fingerprints were imprinted on clay tablets to keep track of business transactions (BIMA, n.d.). From the Babylonian era, biometric identification appears to have been utilized over time in similar ways, but was a not significant commodity until the 1800s.

In the 19th century, individuals were reported to have used hand impressions and fingerprints as an additional method of identification to sign contracts and documents in order to avoid forgery (BIMA, n.d.). Specifically, in 1892, Sir Francis Galton implemented the use of identification of individuals through fingerprints, which led to the creation of the Henry Classification system in 1897. The Henry Classification system allows for an organized method to classify and store fingerprints by assigning individual fingerprints a numerical value based on pattern (Pike, 2013). The creation of the Henry Classification system continued to drive further advancements and increased usage of biometrics.

In the 20th century, The National Bureau of Criminal Identification, Identification Division of the FBI, and forensic organizations were established as law enforcement began to utilize and store fingerprints for criminal identification. Law enforcement has made advancements by using computer technology for fingerprint, iris, speech and voice, face, and hand geometry recognition to not only to identify criminals but also to maintain restricted access in government institutions (BIMA, n.d.). The forensics and law enforcement fields appear to be the primary users of biometrics, but the usage of the identification method continues to proliferate.

The use of biometrics in the 21st century has not only provided security and privacy but also convenience and accuracy in obtaining identification for many agencies, businesses, and consumers. The evolution of biometrics has made the means for identification recognition a more commonly utilized method to manage accessibility of information systems and ensure security with hardware and software-based computer systems (Perrin, 2002). Border control, airports, financial systems, and consumers are a few of the many to take advantage of the advancements made in biometrics, but the identification method seems to be accelerating in the healthcare industry in particular (Find Biometrics, 2013).

Current Applications in Healthcare

As a result of the federal government's mandate for all American health records to be electronic by 2014, biometrics is currently being used as a security approach to maintain the patient privacy laws enforced by the Health Insurance Portability and Accountability Act (HIPAA). Biometrics implements patient privacy and confidentiality, restricts access, and detects fraudulent account access of the EHR (Arnold & Boggs, 2011; Zuniga et al., 2009). Additionally, due to the fact that more patients are receiving care from a variety of healthcare providers and agencies, biometrics controls the likelihood of security breaches as patient information is transferred (Zuniga et al., 2009). By requiring healthcare providers to scan biometric features for authentication and access to the EHR computer systems, security is heightened. In addition, biometric systems are used to discourage impersonation of authorized healthcare providers by notifying delegated authorities of attempts at fraudulent account access of the EHR. A record is kept of individuals

who access or attempt to access to the EHR (Find Biometrics, 2013; Zuniga et al., 2009).

Advantages of Biometrics

Biometric technology delivers various advantages, which make the means of identification in healthcare an effective method for securing the EHR data. First, unlike personal identification numbers and passwords, an individual's biometric features are challenging to replicate, share, or be stolen (Zuniga et al., 2009). Even with the creation of a cloned feature, which impersonates the characteristics of an authorized individual, fraudulent access to the EHR is near to impossible. With the electric-field sensors used in biometrics, the system is able to detect electrical conduction, or measure how much light the finger absorbs, to prove the characteristic belongs to a living person (Jain, 2007). As a result, the system ensures the information submitted and revised in the EHR is done so only by authorized individuals, which makes the accountability of the data more accurate (Zuniga et al., 2009).

In addition, biometrics has been proven to reduce system maintenance costs in comparison to previous methods of security, which require password maintenance, replacing lost or stolen access cards, and reissuing forgotten passcodes (Zuniga et al., 2009). With greater efficiency and reduced maintenance costs, biometric technology appears to be a productive way to secure the EHR. Furthermore, the usability and reduction in overall maintenance costs make the use of biometrics a preferable method to securing the EHR. As far as being user-friendly, biometrics is straightforward and simple, enabling faster authentication and access to patient records in times of emergency.

Disadvantages of Biometrics

On the contrary, the use of biometrics as an approach to secure the EHR in healthcare may also be accompanied by setbacks. For instance, while the total cost of system maintenance is lower, the initial cost of establishing a biometric system is expensive. In general, hospitals use fingerprint scanners as a means to access the EHR, which may cost anywhere between $200 and $1,000 each, depending on quality (Zuniga et al., 2009). Accordingly, the primary investment in biometrics for hospitals and other healthcare settings interested in having the most accurate fingerprint scanners is an expensive price to pay.

Moreover, reading accuracy may be hindered by certain factors when using biometric systems, which can elevate both false acceptance and rejection rates. For example, if the original scan of an individual's biometric feature is inadequate during the enrollment process, the system will not be able to accurately match the scan to the person's template in the future. Inaccurate readings during enrollment or during general use may also be attributed to incorrect placement of the biometric feature or environmental factors, such as temperature, dirt, or humidity. Additionally, when age or injury deteriorates the quality of a biometric feature, the accuracy of the scan is diminished (Zuniga et al., 2009). All factors contributing to false acceptance and rejection rates present risks of breach of confidentiality, increased maintenance costs, and decreased efficiency.

Impact of Biometrics in Healthcare

When introducing biometric technology into healthcare, the acknowledgement of possible sociocultural, ethical, and legal consequences is important. For instance, depending on sociocultural

practices, some individuals may refuse to use a fingerprint scanner due to belief that the frequently touched device could spread disease. Other individuals who have religious beliefs, which consider the scanning of a body part intrusive, would also raise consequences (Pato & Millett, 2010). Moreover, the ethical issue of privacy with biometrics is a concern for certain individuals because the information scanned is a part of identity. Due to the fact that biometrics currently lacks a set of rules to ensure protection of privacy, individuals who have a strong sense of identity may believe autonomy and liberty are threatened (Pato & Millett, 2010). Legal issues which may arise with biometrics include the attempt to impersonate an authorized individual and identity theft, as previously discussed. Another legal issue to consider with biometrics is that when a false rejection occurs, an individual may be denied rights to receive necessary medical care in a timely manner (Pato & Millett, 2010).

Potential Applications of Biometrics in the Future of Healthcare

As biometric technology becomes more prevalent in healthcare to secure the EHR, the recognition mechanism may be the future in patient identification. According to John Trader (2012), The Joint Commission's priority patient safety goal in 2012 was to improve the accuracy of patient identity. As a result, increasing patient safety, as well as reducing liability and medical identity theft in healthcare, has been of focus. Currently, most healthcare settings use insurance cards, date of birth, or bar-coded bracelets for patient identification, which are easily susceptible to fraud. New biometric technology, such as vascular recognition, is one method that can be applied to improve the patient identification process. Vascular recognition captures the pattern of veins in an individual's hand with a near-infrared light. The vascular recognition technology allows for a faster and more accurate method of identification than most current applications (Mackenzie, 2011). Applying biometrics to identification can not only diminish the occurrence of patient fraud but may prevent liability by reassuring care is given to the correct patient, as well as increase efficiency (Trader, 2012).

Conclusion

Overall, the use of biometrics in healthcare has greatly affected the security of the EHR and continues to affect the way healthcare is provided. This identification method which is used for patient recognition has the ability to strengthen the overall security of patient data and confidentiality. However, the disadvantages of biometrics, along with sociocultural, ethical, legal, and fiscal consequences may seem daunting to some individuals. Although the drawbacks of biometrics have been made apparent, keeping in mind the additional applications and future uses of the technology may be a crucial part of health care evolution.

References

Arnold, E.C., Boggs, K.U. (2011). *Interpersonal relationships: professional communication skills for nurses* (6th ed.). Fornango, J., Hayden, M.D., Broeker, M., & Bays, H.D. (eds.). St. Louis, MI: Saunders.

Biometrics Identity Management Agency. (n.d.). *Biometrics history timeline.* Retrieved from http://www.biometrics.dod.mil/References/Biometrics_Timeline.aspx

Find Biometrics. (2013). *Applications.* Retrieved from http://findbiometrics.com/applications/consumerresidential-biometrics/

Jain, A.K. (2007). Technology: biometric recognition. *Nature, 449*. Retrieved from http://search.proquest.com

Mackenzie, K. (2011). Biometric palm reading: the future of patient identification? *Health Leaders Media.* Retrieved from: http://www.healthleadersmedia.com

Pato, J.N., & Millett, L.I. (2010). *Biometric recognition: challenges and opportunities*. Washington, DC: The National Academies Press.

Perrin, R.A. (2002). Biometrics technology adds innovation to healthcare organization security systems. *Healthcare Financial Management, 56*(3). Retrieved from http://search.proquest.com

Pike, J. (2013). History of biometrics. *Biometrics Overview.* Retrieved from http://www.globalsecurity.org/security/systems/biometrics-history.htm

Trader, J. (2012). Biometric patient id technology: is it the future of patient access? *Insightful Coverage of Health Care Innovation.* Retrived from: http://www.hitconsultant.net/2012/10/18/biometric-patient-id-technology-is-it-the-future-of-patient-access/

Zuniga, A.E., Win, K.T., & Susilo, W. (2010). Biometrics for electronic health records. *Journal of Medical Systems, 34*(5). Retrieved from http://search.proquest.com