Optimizing Patient Identity Management in Healthcare: Strategic Recommendations to Implement a Biometric Solution

Anaida Parrilla González
Master of Engineering Management
Dr. Héctor J. Cruzado
Graduate School
Polytechnic University of Puerto Rico

Abstract *— Patient misidentification remains a significant risk in hospital environments, contributing to medical record mismatches, administrative inefficiencies, and treatment delays. Many healthcare facilities continue to rely on traditional identification methods that are vulnerable to duplication and human error. This study evaluates the viability of implementing biometric identification systems in hospitals in Puerto Rico to reduce identification risks, improve operational efficiency, and address regulatory and operational challenges. A literature review of biometric applications in healthcare, analysis of existing implementation cases, and surveys and interviews with patients and medical staff were conducted to assess acceptance, viability, and practical considerations. Results indicate that 68% of respondents perceive the current identification process as inefficient, while clinical and administrative staff report increased errors and delays during high-demand periods. The findings suggest that biometric systems can reduce identification errors, shorten waiting times, and enhance data security. A phased pilot implementation is recommended to support regulatory compliance requirements.*

Key Terms *— Biometric Solutions, Correct Patient Identification, Management Efficiencies, Strategic Healthcare.*

INTRODUCTION

Biometric identification, the process of verifying a person's identity through unique biological characteristics, is a rapidly advancing technology used worldwide. Common modalities such as facial recognition, fingerprint scanning, and iris recognition are applied in areas including mobile authentication, secure access control, and law enforcement. Despite the growth of biometric technologies, many healthcare facilities continue to rely on traditional identifiers such as patient names, insurance numbers, and Social Security numbers, which are vulnerable to errors, duplication, and fraudulent misuse. These limitations contribute to mismatched medical records, delayed treatment, and administrative inefficiencies. Biometric systems offer accurate, secure, real-time access to patient records while reducing reliance on conventional identifiers; critical for delivering safe, effective, and efficient healthcare. Although adoption in healthcare remains limited, some hospitals have begun integrating biometric solutions, particularly benefiting emergency situations involving unconscious or unidentified patients. However, widespread implementation faces challenges, including legacy system integration, privacy compliance, cost management, and user acceptance.

The objective of this study is to develop strategic recommendations for the successful implementation of biometric identification in healthcare facilities in Puerto Rico. These recommendations will address system integration, cost management, user acceptance, and risk mitigation. The main goal is to propose a process that will enhance the patient identification process and management efficiency within the Puerto Rican healthcare system.

METHODOLOGY

This study employed analytic research to develop a set of recommendations to implement biometric identification systems in healthcare facilities in Puerto Rico. An evaluation of existing scientific articles, case studies, and reports was conducted to examine experiences regarding biometric identification systems in healthcare. The

study analyzed selected cases where biometric identification systems had been implemented, such as Geisinger Health. In addition, legal, regulatory, and technical frameworks were analyzed to contextualize the implementation within local constraints. This review aided in the clarification of the implementation of technology in local hospitals.

Interviews were conducted with medical staff to assess their perceptions and attitudes, exploring perceived benefits, concerns, and limitations. Hospital managers and administrative staff were interviewed to provide insights into the viability of these technologies in Puerto Rican hospitals. Potential patients were surveyed regarding their willingness, comfort, trust, and acceptance of biometric identification systems. Ethical standards, including informed consent and confidentiality, were observed throughout the data collection. Quantitative responses were analyzed to identify trends and significant factors influencing acceptance and implementation success. Additionally, qualitative data responses from open questions were examined to extract recurring benefits and concerns among participants.

Finally, the literature review was integrated with survey results to formulate a set of recommendations to implement biometric identification systems in Puerto Rican healthcare facilities. These recommendations were designed to address system integration, risk mitigation, data protection, and user acceptance and provided a practical and realistic framework for future deployments.

LITERATURE REVIEW

Biometrics refers to the technology that recognizes unique physiological or behavioral characteristics [1]. Common modalities include fingerprints, facial recognition, iris scanning, and voice pattern recognition. Unlike traditional identification methods, such as passwords or ID cards, biometrics utilize traits that are inherently difficult to replicate, providing a higher degree of security for access. In today's technological world, precise individual identification is critical [2]. Many applications require the proper and accurate identification of a person. Biometrics are widely used in individuals' daily life, exemplified by widespread use in mobile device authentication. Traditional identification relies on possessions such as ID cards, knowledge such as Social Security numbers or passwords, or a combination of both methods [2]. In contrast, the use of advanced biometric technologies has demonstrated to improve accuracy in sectors ranging from law enforcement to financial services [3].

Biometrics systems are accompanied by several challenges and concerns. From the perspective of user experience, studies have shown that participants express concerns regarding security and biometric data handling [4]. Such concerns reflect a degree of mistrust among some users who may request biometric authentication, highlighting the importance of transparency in healthcare implementations. Medical conditions including burnt skin, ocular damage, and other physiological impairments pose significant challenges [1]. Fraser identifies contemporary issues related to biometrical technologies, such as bias in recognition based on race, age, and gender [5]. Regulatory and ethical consideration, including compliance with HIPAA and the necessity for informed patient consent further represents persistent challenges.

In healthcare, biometric systems are used primarily to improve patient identification, data security, and administrative efficiency. Patient misidentification has been associated with medical errors, record duplication, and operational inefficiencies in medical facilities. In cases of emergency, medical professionals often identify an unconscious patient as Jane or John Doe until they can be identified [6]. Biometric technologies effectively identify individuals. Moreover, evidence indicates that identification systems can accurately identify patients with minimal errors and high completion rates [7]. Biometrics also contributes to the protection of healthcare electronic records, reducing medical risks and fraud. This form of authentication provides additional security regarding

data breaches, adding a security layer compared to a password, which can safeguard access to restricted areas, including those controlling medical devices and sensitive medications [8].

Geisinger Health in Pennsylvania has implemented effectively biometrical identification for their patients [9]. Using Certify Health, a brand set to improve innovation at healthcare facilities, Geisinger Health is set to continue expanding the implementation of throughout their health systems, integrating seamlessly with their Electronic Health Record (EHR) [10]. The process for patient identification is simple for both the administrative staff and the patient. During their first visit, a patient is photographed for biometric record. This biometric data is attached to the patient's record. Using this method, patients at Geisinger Health have more control over their health data. The future of electronic health records emphasizes a shift toward more patient-centered and consumer-driven systems in which individuals have greater control over their health information [11]. Emerging EHR models are designed to improve transparency, accessibility, and user experience, enabling patients to interact more directly with their data while maintaining security and privacy protections [11].

Discussion of Survey Findings

The survey for potential patients showed that most respondents reported familiarity with biometric technologies. Figure 1 presents respondents' perceptions of the time required to complete the current patient identification process. The results show that 79% of participants reported identification times exceeding five minutes, suggesting that the existing process may introduce critical delays, particularly in emergency situations where rapid access to patient information is essential. These delays are increased during busy periods, increasing operational inefficiency and potential clinical risk.

As shown in Figure 2, 68% of respondents perceived the current patient identification process as imprecise. This perception indicates vulnerability to errors that may lead to patient misidentification and reinforces concerns regarding the reliability of existing identification procedures.

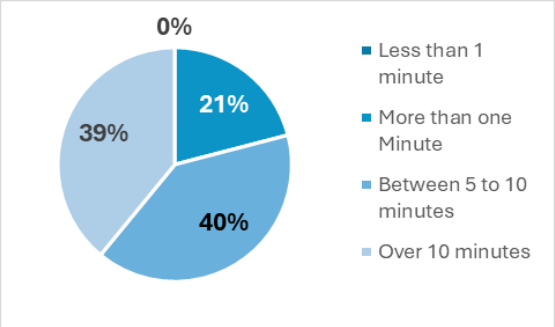

Figure 1
Time Perceived by Respondents Through the Actual Identification

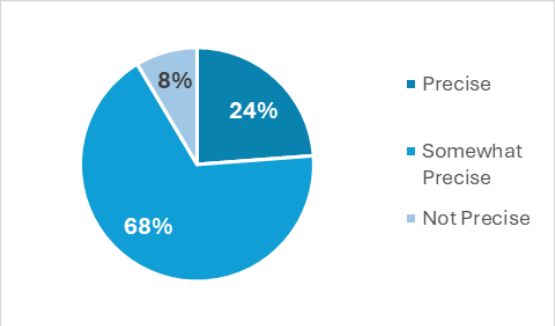

Figure 2
Experienced Precision of Actual Process by Respondents

Figure 3 illustrates respondents' preferences regarding the implementation of biometric identification systems. The results indicate that 49% of participants favored biometric identification as an optional system rather than a complete replacement of existing methods, reflecting concerns related to trust, familiarity, and perceived risks. This indicates that a hybrid approach may be more effective during early stages which facilitates user confidence, reduces resistance and support transition while maintaining operations.

Concerns regarding the protection and security of biometric data were consistently raised, underscoring the importance of robust privacy safeguards. Overall, these findings highlight operational limitations in the current patient identification system and indicate that a phased or hybrid implementation would improve user acceptance while minimizing risk.

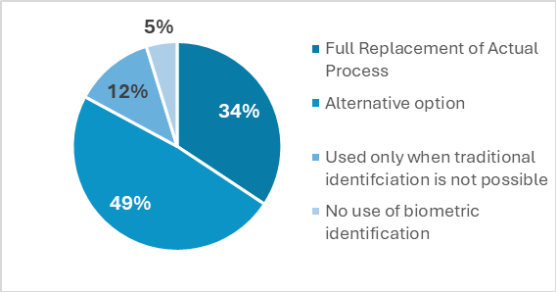

Figure 3
Respondents Opinions on Using Biometrics Identification in Health

Interviews with medical and administrative staff revealed that the current identification process relies on physical identification documents, insurance cards, and manually-entered patient information. Staff reported experiencing errors, although infrequent, as well as delays during high-volume periods. Additional delays were noted in cases involving patients with preexisting conditions or complications from prior procedures. Concerns were also expressed regarding system reliability during power outages or system failures.

Traditional documentation-based identification is inefficient in emergency situations where patients cannot self-identify. Digitally integrated biometric systems can reduce identification time, improve consistency, and limit human error, particularly in high-volume and time-critical settings where mistakes may have severe consequences. Privacy and data protection are fundamental to biometric implementation. Puerto Rico Law 40-2012 [12] requires secure electronic health records linked to a unique patient identity, aligning with biometric capabilities when properly governed. Since healthcare facilities already use compliant electronic record systems, biometrics can enhance existing infrastructure without requiring full system replacement.

RECOMMENDATIONS

It is recommended that the implementation of a biometric system coordinated among participating healthcare facilities be facilitated through the Puerto Rico Department of Health. The Department's role should focus on defining operational standards, governance policies, and compliance requirements to support secure identity verification across emergency care facilities. This centralized coordination would promote consistency while allowing hospitals to retain control over their internal systems and patient data. Privacy and regulatory compliance must be embedded into the system design from the outset. Biometric data handling should comply with applicable federal regulations and Puerto Rico Law No. 40-2012, requiring secure storage, controlled access, and auditable system activity. Implementing federated or decentralized identity-matching architectures can further minimize data exposure by limiting the exchange of identifiable biometric information across institutions.

It is further recommended that the initial implementation of biometric identification systems be limited exclusively to emergency departments, where the highest operational risk for patient misidentification exists due to time-critical decision-making, high patient volume, and frequent cases in which patients are unable to self-identify. Biometric identification should be implemented as an integrated component of existing electronic health record systems rather than as a standalone platform. Many hospitals in Puerto Rico already operate electronic systems that comply with federal and local regulatory requirements. Integrating biometric functionality into existing infrastructure avoids duplication of patient records, reduces implementation complexity, and leverages established clinical workflows. A hybrid identification approach should be adopted to complement, rather than replace, traditional identification methods. Maintaining conventional identification options ensures continuity of care when biometric verification is unavailable or impractical, while supporting gradual user acceptance and reducing resistance to adoption among patients and staff. Moreover, hybrid systems enhance reliability during emergency situations involving power outages or system failures.

Prior to broader adoption, a controlled pilot program should be conducted in selected emergency departments where electronic systems are already in place. This pilot phase should evaluate performance indicators such as identification time reduction, system reliability, staff acceptance, and compliance with privacy requirements. The results of this evaluation should inform future decisions regarding system refinement and potential expansion beyond emergency care, as well as broader implementation across the island.

Conclusion

The adoption of biometric identification in Puerto Rico's healthcare system presents a strategic opportunity to reduce patient misidentification, particularly in emergency settings where accuracy and timeliness are critical. A phased, governance-driven implementation coordinated by the Puerto Rico Department of Health can balance innovation with operational feasibility, regulatory compliance, and patient privacy while maintaining institutional autonomy. Focusing initial deployment in emergency departments and integrating biometrics into existing electronic health record systems minimizes disruption, supports interoperability, and improves workflow continuity. Hybrid identification models enhance system resilience and user acceptance during operational contingencies. Implementing a controlled pilot program is essential to validate performance, assess impact, and guide scalable, sustainable adoption. Together, these measures provide a practical and risk-conscious framework for strengthening patient identity management while preserving trust and clinical effectiveness.

References

[1] Nait-Ali, A. (2018). Biometrics under biomedical considerations (eText ISBN: 9789811311444). Springer Nature Singapore.

[2] Marana, Aparecido & Falguera, Juan & Jain, Anil & Sartori Falguera, Fernanda. (2006). Biometrics for Human Identification. RITA. 103-130.

[3] Haley P. The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent. Sensors (Basel). 2025 May 17;25(10):3160. doi: 10.3390/s25103160. PMID: 40431950; PMCID: PMC12116099.

[4] Hussaini, B. (2024, June 16). Risks and challenges associated with biometric *authentication in multifactor authentication systems* (Bachelor's thesis, School of Engineering, Jönköping University, Jönköping, Sweden).

[5] Fraser, M. O. (2024, February 12). Taking a closer look: Assessing biometric *authentication*. *Health Law Journal*, *29*(1). New York State Bar Association. Retrieved from https://nysba.org/taking-a-closer-look-assessing-biometric-authentication/

[6] Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., & Roy, K. (2020). An investigation of biometric authentication in the healthcare environment. Array, 8, Article 100042. https://doi.org/10.1016/j.array.2020.100042

[7] Sohn, J. W., Kim, H., Park, S. B., Lee, S., Monroe, J. I., Malone, T. B., Kinsella, T., Yao, M., Kunos, C., Lo, S. S., Shenk, R., & Machtay, M. (2020). Clinical Study of Using Biometrics to Identify Patient and Procedure. *Frontiers in oncology*, *10*, 586232. https://doi.org/10.3389/fonc.2020.586232

[8] An Y. Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards. J Biomed Biotechnol. 2012;2012:519723. doi: 10.1155/2012/519723. Epub 2012 Jul 31. PMID: 22899887; PMCID: PMC3415263.

[9] CERTIFY.me. (2021, September 29). *Geisinger utilizes CERTIFY facial recognition*. CERTIFY.me. Retrieved from https://www.certify.me/blog/certify-health-expands-biometric-positive-patient-id-with-geisinger/

[10] CERTIFY Health. (2021, June 3). *CERTIFY Health expands biometric positive patient ID with Geisinger* [Press release]. PR Newswire. Retrieved from https://www.prnewswire.com/news-releases/certify-health-expands-biometric-positive-patient-id-with-geisinger-301305365.html?

[11] Sterrett, L., Harris, C., Batra, N., Talbot, C., Chang, C., & Malhotra, R. (2022, October 19). *Preparing for the next generation of electronic health records*. Deloitte Insights. Retrieved from https://www.deloitte.com/us/en/insights/industry/health-care/ehr-systems-the-future-of-electronic-health-records.html

[12] Asamblea Legislativa de Puerto Rico. (2012). Ley Núm. 40-2012, Ley para la administración e intercambio electrónico de información de salud en Puerto Rico. Estado Libre Asociado de Puerto Rico.