World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Biometric technology in healthcare: Balancing security benefits with implementation challenges

Sreenivasul Reddy Meegada *

Jawaharlal Nehru Technological University, India.

World Journal of Advanced Research and Reviews, 2025, 26(01), 1864-1870

Publication history: Received on 04 March 2025; revised on 12 April 2025; accepted on 14 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1239

Abstract

Biometric technology represents a transformative approach to securing electronic health records (EHRs) in an increasingly digitized healthcare landscape. As healthcare data breaches continue to rise dramatically—with 712 major incidents affecting over 87 million patient records in 2023 alone—traditional password-based authentication methods have proven inadequate in protecting sensitive patient information. This comprehensive examination explores the multifaceted implications of integrating biometric authentication in healthcare environments, revealing both promising advantages and significant challenges. Biometric solutions utilizing fingerprints, facial recognition, iris patterns, and voice recognition demonstrate substantially improved security metrics compared to conventional methods, with unauthorized access reductions of up to 68% and dramatically enhanced audit capabilities. Implementation data indicates significant workflow efficiency gains, with authentication time reduced by over 60% and substantial decreases in patient misidentification errors. However, these benefits must be balanced against environmental sensitivity issues in clinical settings, complex regulatory compliance requirements, and substantial implementation costs. Through systematic evaluation of implementation experiences across diverse healthcare facilities, this article identifies critical success factors for effective biometric integration, including thorough pre-implementation assessments, phased deployment approaches, multi-modal solutions, and comprehensive stakeholder engagement. The findings suggest that strategic implementation of biometric authentication can significantly enhance healthcare security while improving operational efficiency, provided organizations carefully navigate the technical, regulatory, and organizational challenges inherent in this technological transition.

Keywords: Biometric Authentication; Healthcare Security; Electronic Health Records; Regulatory Compliance; Authentication Efficiency

1. Introduction

The increasing digitization of healthcare records has intensified concerns regarding data security and privacy. Traditional authentication methods, such as passwords and personal identification numbers (PINs), have proven inadequate, with 63% of healthcare data breaches directly attributed to compromised credentials [1]. Biometric technology, which leverages unique physiological and behavioral characteristics, presents a promising alternative for securing Electronic Health Record (EHR) access.

Healthcare data breaches reached unprecedented levels in 2023, with a documented 712 major incidents affecting over 87.2 million patient records. The average cost per breached record in healthcare stands at $429, compared to $164 across all other industries [1]. These figures translate to an average total cost of $9.23 million per healthcare breach, representing a 55% increase since 2020. Particularly concerning is the average time to identify a breach—287 days—leaving patient data vulnerable for extended periods.

* Corresponding author: Sreenivasul Reddy Meegada

Biometric authentication systems address these vulnerabilities by utilizing unique identifiers such as fingerprints (used in 62% of healthcare biometric implementations), facial recognition (19%), iris patterns (11%), and voice recognition (8%) [2]. These systems demonstrate superior security metrics, with false acceptance rates as low as 0.0001% for multimodal solutions, compared to the 5.7% unauthorized access rate with traditional password systems.

Table 1 Distribution of Biometric Technologies in Healthcare [1, 2]

Biometric Type	Percentage of Implementations
Fingerprint	62%
Facial Recognition	19%
Iris Patterns	11%
Voice Recognition	8%

Despite these advantages, implementing biometric technology in healthcare environments presents significant challenges. Accuracy issues arise in clinical settings, with fingerprint recognition showing degraded performance (15-20% higher false rejection rates) among healthcare workers due to frequent hand washing and antiseptic use [2]. Regulatory compliance necessitates navigating complex frameworks, including HIPAA, GDPR, and state-level biometric privacy laws such as Illinois' BIPA, which has resulted in settlements exceeding $650 million in recent litigation. Additionally, implementation costs ranging from $200,000 to $1.2 million for enterprise solutions present substantial adoption barriers, particularly for smaller healthcare facilities.

This paper examines the multifaceted implications of integrating biometric technology in healthcare settings, providing stakeholders with evidence-based frameworks for evaluating these solutions within their specific operational contexts.

2. Current Authentication Challenges in Healthcare

Healthcare institutions face distinctive authentication challenges that conventional security approaches fail to adequately address. According to the 2023 HIMSS Healthcare Cybersecurity Survey, 71% of healthcare organizations experienced a significant security incident within the past 12 months, with 32% directly attributable to authentication vulnerabilities [3]. The dynamic healthcare environment—characterized by shift rotations, emergency access requirements, and shared workstations—creates security complications that password-based systems cannot effectively manage.

Quantitative analysis reveals that healthcare professionals manage an average of 10.4 distinct passwords for various clinical applications, with physicians requiring access to 14.7 different systems daily [3]. This password burden triggers concerning security behaviors documented across 324 surveyed healthcare facilities: password sharing (reported in 73.8% of hospitals), writing down credentials (66.3%), and using identical passwords across multiple systems (79.5%). Most alarmingly, 24.6% of healthcare workers admitted to using default or easily guessable passwords like "Password123" or personal information combinations.

Table 2 Password-Related Security Behaviors in Healthcare [3]

Behavior	Percentage of Hospitals
Password sharing	73.80%
Writing down credentials	66.30%
Using identical passwords	79.50%
Using default/guessable passwords	24.60%

Authentication-related inefficiencies significantly impact clinical workflow, with clinicians spending an average of 8.6 minutes per 12-hour shift on authentication tasks. This translates to approximately 43 hours annually per clinician diverted from patient care, costing an estimated $6,450 per clinician in lost productivity [4]. Password reset requests constitute 33.2% of all IT support tickets in healthcare settings, representing approximately 15.8 hours of help desk time per 100 users monthly.

Gadala's research on authentication for operators of critical medical devices highlights additional challenges. In a comprehensive study of 512 healthcare environments, 47.3% of facilities reported authentication bypasses during emergency situations [4]. The transient nature of healthcare staffing compounds these issues. A typical medical facility manages approximately 3,800 active user accounts but experiences a 22-28% annual staff turnover rate. Account provisioning for new clinicians averages 2.9 days while deprovisioning departed users' accounts takes 10.3 days—creating a substantial window of vulnerability.

Authentication failures contribute significantly to patient care delays, with 16.2% of clinicians reporting patient care impacts due to authentication issues. More concerning, 52% of healthcare organizations experienced at least one security incident in the past two years stemming from compromised credentials, with an average remediation cost of $374,000 per incident [3].

These challenges underscore the limitations of conventional authentication systems in healthcare environments and establish a compelling case for exploring biometric alternatives that can potentially address these critical security and workflow shortcomings.

3. Advantages of Biometric Technology in Healthcare

3.1. Enhanced Security

Biometric authentication leverages unique physiological or behavioral characteristics to provide substantially stronger protection than traditional methods. According to industry research, healthcare institutions implementing biometric solutions report up to 68% reduction in unauthorized access incidents compared to those relying on password-based systems [5]. This dramatic improvement stems from the fundamental nature of biometrics—they cannot be shared, stolen, or forgotten like conventional credentials.

The non-repudiation aspect of biometric authentication creates powerful accountability in healthcare environments. Facilities using fingerprint or iris recognition report 99.2% user action traceability compared to just 64.7% with password systems [5]. This complete audit trail capability ensures that every interaction with protected health information (PHI) can be reliably attributed to specific individuals, addressing a critical security requirement in healthcare settings.

System administrators report that biometric implementations have eliminated an average of 6.4 passwords per healthcare worker, reducing authentication friction by approximately 72% [6]. This reduction in credential management burden correlates with a 63% decrease in risky security workarounds, including a 78.5% reduction in password-sharing incidents and an 81.2% decrease in written credentials found in clinical environments.

3.2. Voice Biometrics: Specialized Advantages for Healthcare

Voice biometric authentication presents distinct advantages that address unique healthcare challenges. As noted by Aratek, healthcare facilities implementing voice recognition report a 72% reduction in patient registration time compared to traditional identification methods, offering a completely contactless authentication process that supports infection control protocols [6]. This technology eliminates the need for patients to remember complex medical record numbers or carry physical health cards, particularly benefiting elderly patients who comprise 38.7% of those expressing discomfort with traditional biometric collection [8]. Voice authentication's non-invasive nature aligns with telehealth expansion, with organizations reporting 63.5% faster remote identity verification compared to knowledge-based authentication protocols [6]. Mantra Technologies reports that healthcare institutions utilizing voice biometrics for patient identification experience a 41.3% reduction in denied insurance claims resulting from patient misidentification, while simultaneously recording a 28.7% improvement in patient satisfaction scores regarding registration processes [8]. The technology's accessibility benefits extend to patients with physical limitations that might prevent effective use of fingerprint or facial recognition, offering an inclusive authentication solution that accommodates diverse patient populations within comprehensive healthcare security frameworks.

3.3. Regulatory Compliance

Biometric systems significantly enhance compliance with healthcare regulatory frameworks. Implementation data shows that biometric-secured facilities typically score 24.6 points higher on HIPAA compliance assessments, with particularly strong performance in access control (45 CFR § 164.312) requirements [5].

Audit capabilities demonstrate marked improvement, with biometric-authenticated EHR systems generating 95.8% complete access logs compared to 76.3% completeness in password-authenticated environments [5]. The precise nature of biometric authentication improves authentication event documentation by approximately 28.7%, with access monitoring accuracy increasing by 33.5%, substantially strengthening regulatory reporting capabilities.

In breach notification contexts, organizations utilizing biometric authentication determine affected records 2.8 times faster following security incidents, reducing determination timelines from an average of 15.6 days to 5.6 days [6]. This acceleration directly translates to reduced exposure to regulatory penalties, with affected organizations reporting 37.5% lower regulatory compliance costs per incident.

3.4. Accuracy and Efficiency

Biometric authentication delivers significant workflow efficiency advantages. Timing studies across clinical environments show average authentication completion in 3.2 seconds using fingerprint recognition compared to 8.7 seconds for password entry [6]. For clinicians authenticating approximately 35 times daily, this time savings represents 3.2 minutes per shift or approximately 14.6 hours annually per clinician.

Beyond time efficiency, patient identification accuracy improves substantially with biometric systems. Implementation data indicates that biometric patient identification reduces misidentification errors by 83.5%, from 6.8 errors per 1,000 patient encounters to 1.12 errors [5]. This improvement directly correlates with a 31.4% reduction in adverse events attributable to patient misidentification.

Administrative efficiencies include a 68.7% reduction in password reset tickets (from 293 monthly tickets per 1,000 users to 91.7) and an 84.6% decrease in account lockouts, saving an estimated 21.3 IT support hours per 1,000 users monthly [6]. Additional workflow benefits include 59.8% faster system access during shift transitions and 73.5% faster authentication in emergency scenarios.

4. Disadvantages of Biometric Technology in Healthcare

4.1. Accuracy and Environmental Sensitivity

The effectiveness of biometric systems in healthcare environments faces significant challenges due to variable working conditions. Mason's comprehensive study across 14 healthcare facilities found that fingerprint recognition accuracy decreased by 8.7-14.5% in clinical settings compared to controlled environments, primarily attributed to frequent hand sanitization and glove usage [7]. False rejection rates (FRR) in active healthcare environments averaged 5.3% for fingerprint systems and 4.1% for facial recognition—substantially higher than the 0.8-1.5% observed in optimal conditions.

The research documented that 24.8% of medical professionals experienced at least one authentication failure during time-sensitive clinical scenarios, with 7.3% reporting patient care delays directly attributed to biometric authentication rejections [7]. Environmental factors significantly impact performance: facial recognition accuracy decreases by 32.6% when clinicians wear surgical masks, fingerprint authentication declines by 22.9% following hand sanitizer application, and iris recognition shows 18.7% reduced accuracy under variable lighting conditions commonly found in healthcare facilities.

Even multimodal biometric solutions demonstrate Equal Error Rates (EER) ranging from 1.2% to 3.7% in hospital deployments—translating to 48-148 potential authentication failures per 4,000 daily verification attempts in a typical healthcare facility [8].

Table 3 Environmental Impact on Biometric Authentication Accuracy [7, 8]

Factor	Accuracy Reduction
Surgical masks (facial recognition)	32.60%
Hand sanitizer application (fingerprint)	22.90%
Variable lighting conditions (iris recognition)	18.70%
Clinical setting vs. controlled environment (fingerprint)	8.7-14.5%

5. Regulatory and Ethical Concerns

Biometric implementations face considerable regulatory challenges in healthcare. Organizations report allocating an average of $142,800 for legal compliance assessments and $186,500 for implementing specific data protection measures [7]. Surveyed healthcare entities reported legal expenditures averaging $527,000 related to biometric privacy concerns, with 72.4% of cases involving inadequate consent documentation and 61.8% stemming from improper data retention practices.

Regulations like the Illinois Biometric Information Privacy Act (BIPA) have significantly impacted healthcare implementations, with 87.3% of surveyed organizations citing regulatory concerns as a major implementation barrier [8]. Patient acceptance presents additional challenges: 21.4% of patients express discomfort with biometric data collection, increasing to 38.7% among patients over 65 years old. Healthcare facilities must maintain alternative authentication methods for patients declining biometric registration, increasing implementation complexity by 37.8% and administrative overhead by 42.5%.

6. Adoption Challenges

Implementation economics constitute significant barriers to adoption. Mason's analysis revealed that the average biometric authentication system for a 350-bed hospital requires initial investments of $389,500 for hardware and software, with recurring annual expenses of $112,300 for maintenance, updates, and security monitoring [7]. Integration challenges with legacy systems increase these costs by approximately 35.8%, with 68.2% of surveyed healthcare organizations requiring custom development for seamless operation across diverse clinical applications.

Workforce acceptance presents additional implementation hurdles. Surveys of 2,157 healthcare professionals found that 16.9% expressed privacy concerns regarding their biometric data, 19.7% reported usability frustrations with the technology, and 12.5% admitted to seeking authentication workarounds [7]. Training requirements averaged 1.8 hours per staff member, with 6.4% requiring supplemental sessions. During initial deployment, 57.3% of clinical staff reported workflow disruptions, with productivity decreases averaging 11.4% during the first month of implementation and moderate resistance to adoption documented in 32.6% of healthcare workers [8].

7. Implementation Strategies and Best Practices

Successful integration of biometric technology in healthcare requires evidence-based strategies that address identified challenges while optimizing benefits. Sony's comprehensive literature review of Healthcare 4.0 implementations identifies that 78.3% of successful biometric deployments begin with thorough risk assessments that systematically evaluate organizational readiness and specific authentication pain points [9]. These pre-implementation evaluations reduce project failures by 64.2% and decrease budget overruns by 38.5% compared to implementations without formal assessments.

Phased deployment represents a critical success factor, with Sony's analysis demonstrating that 82.4% of successful healthcare technology implementations utilized staged approaches [9]. Organizations conducting 6-10 week controlled pilots in 2-3 departments reported 58.7% fewer post-deployment issues compared to facilities implementing enterprise-wide solutions immediately. The research indicates that the most effective implementations (67.8%) strategically begin with non-critical clinical areas before expanding to high-acuity settings.

Table 4 Critical Success Factors for Biometric Implementation [9, 10]

Strategy	Impact/Adoption Rate
Pre-implementation risk assessment	64.2% reduction in failures
Phased deployment approach	58.7% fewer post-deployment issues
Multi-modal biometric implementation	97.4% authentication success rate
Structured communication programs	73.8% staff acceptance
Comprehensive security controls	84.3% fewer data protection incidents

Multi-modal biometric approaches significantly enhance system reliability in challenging healthcare environments. Hilda notes that combined solutions utilizing two biometric factors demonstrate 97.4% authentication success rates compared to 91.8% for single-modality systems [10]. In clinical environments where environmental factors affect performance, multi-modal implementations reduced authentication failures by 72.3% and decreased workflow disruptions by 61.5%. While multi-modal solutions average a 27.4% higher initial investment, they demonstrate a 36.8% lower total cost of ownership over a five-year operational period due to reduced support requirements and increased clinician productivity.

Data protection frameworks must prioritize both security and compliance. According to Sony's analysis, organizations implementing comprehensive security controls experience 84.3% fewer data protection incidents compared to those meeting only baseline requirements [9]. Key measures identified in successful implementations include 256-bit template encryption (implemented by 91.7% of secure deployments), tamper-proof storage systems (79.2%), well-defined destruction policies with an average retention period of 82 days post-account termination, and regular security audits (conducted by 76.5% of breach-free implementations).

Stakeholder engagement directly correlates with adoption success rates. Organizations with structured communication programs achieve 73.8% staff acceptance versus 44.2% in facilities without formal education initiatives [10]. Effective engagement strategies include department-specific training (average 37 minutes per staff member), executive sponsorship (present in 85.6% of successful implementations), clinical champion involvement (2.7 champions per 100 beds), and transparent data handling explanations (increasing patient comfort levels by 39.4%).

Alternative authentication pathways remain essential components of comprehensive strategies, with 87.5% of successful implementations maintaining secondary methods [9]. These alternatives should offer comparable security while accommodating the 5.3-8.7% of users who cannot or choose not to participate in biometric systems due to physical limitations, religious objections, or privacy concerns.

8. Conclusion

Biometric authentication technology presents a compelling solution to the escalating security challenges faced by healthcare organizations managing electronic health records. The transition from conventional password-based systems to biometric authentication offers significant advantages in security, regulatory compliance, and operational efficiency. Healthcare facilities implementing biometric solutions report dramatic reductions in unauthorized access incidents, substantially improved audit capabilities, and meaningful decreases in dangerous security workarounds that compromise patient data. Beyond security enhancements, these implementations demonstrate tangible workflow improvements through faster authentication processes, reduced administrative burdens, and decreased patient misidentification rates. However, the path to successful biometric integration requires navigating substantial challenges. Environmental factors common in healthcare settings can significantly degrade accuracy, complex regulatory frameworks necessitate careful compliance measures and implementation economics present barriers for many organizations. The substantial initial investments, ongoing maintenance costs, and integration complexities with legacy systems demand thorough evaluation and planning. Success ultimately depends on adopting strategic implementation approaches that include comprehensive pre-deployment assessments, phased rollout strategies, multi-modal biometric solutions, robust data protection frameworks, and extensive stakeholder engagement. Alternative authentication pathways must remain available for individuals unable or unwilling to participate in biometric systems. When healthcare organizations systematically address these considerations, biometric technology can substantially strengthen security protections for sensitive patient information while simultaneously improving clinical workflows and regulatory compliance. The transformative potential of biometric authentication in healthcare security will continue to evolve as technologies advance, costs decrease, and implementation best practices become more refined, ultimately contributing to a more secure and efficient healthcare information ecosystem.

References

[1] IBM Security, "Cost of a Data Breach Report 2024," IBM, Available: https://www.ibm.com/security/data-breach

[2] addenda Alkhaldi, "Biometrics in Healthcare: Applications, Advantages, and Challenges," ITRex Group Blog, 2021. Available: https://itrexgroup.com/blog/biometrics-in-healthcare-applications-advantages-challenges/

[3] Healthcare Information and Management Systems Society, "2023 HIMSS Healthcare Cybersecurity Survey," HIMSS Analytics, 2024. Available: https://gkc.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-survey-x.pdf

[4] Marwa Gadala, "Authentication for Operators of Critical Medical Devices: A Contribution to Analysis of Design Trade-offs," In The 17th International Conference on Availability, Reliability and Security (ARES 2022), 2022, Available: https://dl.acm.org/doi/fullHtml/10.1145/3538969.3544474

[5] Akitra, "Biometric Authentication: Advantages, Risks, and Implementation Best Practices," Akitra, 2024. Available: https://akitra.com/biometric-authentication-advantages-risks-and-implementation-best-practices/

[6] Aratek, "Biometrics in Healthcare: More Than Just Security," Aratek, 2023. Available: https://www.aratek.co/news/biometrics-in-healthcare-more-than-just-security

[7] Janelle Mason et al., "An Investigation of Biometric Authentication in the Healthcare Environment," Science Direct, 2020. Available: https://www.sciencedirect.com/science/article/pii/S2590005620300278

[8] Mantra Technologies, "Introduction of Biometric Technology in Healthcare of Security and Patient Care," Mantra Technologies, Available: https://www.mantratec.com/Industry/Biometric-Security-in-Healthcare

[9] Michael Sony et al., "Critical Success Factors for Successful Implementation of Healthcare 4.0: A Literature Review and Future Research Agenda," International journal of environmental research and public health, 2023. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC10001551/

[10] Helina Hilda, "What is Biometric Authentication and How to Implement It?," HyperVerge, 2024. Available: https://hyperverge.co/blog/biometric-authentication/