# Biometric Authentication and Robot Access Control for Secure Health Devices

**Author:** Rodrigo Torres **Affiliation:** Department of Computer Science, Pontifical Catholic University of Chile (Chile) **Email:** rodrigo.torres@uc.cl

## Abstract

Medical devices and healthcare robots are increasingly networked, making robust authentication and fine-grained access control essential to patient safety, privacy, and regulatory compliance. This article provides an extended, interdisciplinary review of biometric authentication modalities and access-control mechanisms for robotic and Internet-of-Medical-Things (IoMT) devices, synthesizes the threat landscape, and proposes a layered, privacy-preserving framework for **biometric-enabled robot access control (BERAC)** suitable for clinical deployments. We examine physiological and behavioral biometrics (fingerprint, face, iris, electrocardiogram/photoplethysmography, gait, keystroke), continuous and adaptive authentication, cryptographic and hardware protections, role- and context-aware access control models for robots, and system-level considerations including latency, survivability, fail-safe behavior, and regulatory compliance (NIST, FDA). We conclude with privacy, ethical, and implementation guidelines for designers, vendors, and hospitals.

*Keywords: biometric authentication; healthcare robotics; IoMT; access control; NIST; FDA; continuous authentication; privacy; secure medical devices*

## 1. Introduction

The adoption of networked medical devices and healthcare robots—ranging from bedside assistants and medication-delivery robots to remote telepresence and surgical robots—has accelerated in the last decade. These systems promise efficiency and improved care, but also enlarge the attack surface for unauthorized access, data exfiltration, and safety-critical manipulation (e.g., actuator hijack) that may endanger patients. Contemporary literature highlights the susceptibility of Internet-of-Medical-Things (IoMT) devices to diverse cyber threats, motivating stronger identity and access controls tied to both human users and robotic endpoints.

This paper addresses an urgent applied research question: **How can biometric authentication be integrated with robust, context-aware access control for healthcare robots and medical devices while preserving privacy and meeting regulatory guidance (NIST, FDA)?** We present a systematic literature synthesis, threat analysis, design framework (BERAC), and practical evaluation plan.

## 2. Background and Motivation

### 2.1. The expanding attack surface of IoMT and healthcare robots

IoMT and robotic endpoints commonly incorporate embedded sensors, wireless connectivity, and cloud services for telemetry and analytics. This connectivity creates opportunities for remote exploitation;

documented reviews and surveys have repeatedly found IoMT devices suffer widespread vulnerabilities (weak authentication, unpatched firmware, insecure protocols), which can lead to patient harm and data breaches.

### 2.2. Authentication in healthcare: constraints and requirements

Authentication for clinical devices differs from consumer contexts: it must be fast, minimize clinician cognitive load, survive stressful conditions, work with gloves or PPE, and degrade gracefully (allow safe fallback) when sensors or networks fail. It must also support auditability, least-privilege access, and emergency overrides consistent with clinical workflows and regulatory requirements (FDA premarket cybersecurity expectations, NIST identity assurance guidance) (Fatunmbi, 2022).

## 3. Literature Review

This review synthesizes literature across biometric authentication, continuous/adaptive authentication, robotics access control, IoMT security, privacy-preserving biometrics, and human factors.

### 3.1. Biometric modalities in healthcare contexts

- **Physiological biometrics (fingerprint, face, iris):** Widely used in access control; systems must account for occlusion, PPE, and spoofing risks. Facial recognition in clinical settings faces accuracy drops due to masks and lighting; iris scanners provide strong entropy but require user cooperation and optical hardware.
- **Bio-signal biometrics (ECG, PPG):** Emerging evidence supports using cardiac waveforms (ECG) and photoplethysmography (PPG) as liveness and identity signals—especially valuable for continuous authentication on wearables. Recent reviews show PPG-based authentication is promising for non-contact and continuous verification.
- **Behavioral biometrics (gait, keystroke, touchscreen dynamics):** Provide continuous, passive authentication but raise concerns about variability and bias; useful for multi-factor or continuous systems when combined with physiological or cryptographic factors.

### 3.2. Continuous and adaptive authentication

Continuous authentication (CA) monitors identity over time and is particularly useful when devices are shared or when a robot accepts commands over a session. CA approaches based on multimodal fusion (physiological + behavioral + device telemetry) demonstrate improved resilience against replay and mimicry attacks. Key designs trade off detection latency against false alarm rates, especially in clinical tasks where false lockouts are hazardous.

### 3.3. Robot access control models

- **Role-based access control (RBAC):** Common in healthcare informatics; maps well to clinician roles but often lacks contextual nuance for robots (e.g., spatial proximity, patient consent, device state). (Fatunmbi, 2024)
- **Attribute- and context-aware access control (ABAC/CAP):** Emerging work recommends ABAC or context-aware RBAC for robots, integrating attributes like device health, location, clinician certification, time-of-day, and patient consent level to derive dynamic policies. Fine-grained access control is essential for safely constraining robot actuation. (Fatunmbi, 2022)

### 3.4. Cryptographic and hardware protections

Secure enclaves, Trusted Platform Modules (TPMs), hardware-backed biometrics, and secure boot chains mitigate tampering and credential exfiltration. End-to-end cryptography for telemetry and authenticated command channels is necessary. However, constrained embedded devices often require lightweight crypto and careful key management across lifecycle stages.

### 3.5. Privacy, bias, and ethics

Biometric data are sensitive: storage and processing choices (on-device vs. cloud), template protection (cancellable biometrics, secure sketches), and differential privacy approaches are widely studied. Behavioral biometrics raise additional bias concerns—algorithms may underperform for certain demographic groups—necessitating fairness audits. Several reviews call for privacy-preserving multimodal pipelines and human-centered evaluations.

### 3.6. Regulatory and standards landscape

NIST digital identity guidance and FDA cybersecurity expectations frame acceptable practices for identity assurance and medical-device cybersecurity. Recent FDA guidance emphasizes documentation of cybersecurity risk management, resilience, and secure software lifecycle—requirements that influence design and validation of biometric systems in medical devices.

## 4. Threat Model and Security Objectives

### 4.1. Threat model

We consider adversaries with goals of unauthorized control of robotic actuators, data exfiltration from medical devices, denial-of-service (DoS) during care, and privacy compromise of biometric templates. Attack vectors include network-level exploits, replay/spoofing of biometric data, insider abuse, firmware tampering, and supply-chain attacks. We assume adversaries may have local network access (e.g., compromised hospital VLAN) or remote internet access depending on device exposure.

### 4.2. Security objectives

1. **Authentication:** Bind a human identity or authorized process to robot control commands with high assurance.

2. **Authorization:** Enforce least-privilege, context-aware access to robot functions (navigation, medication handling, clinical interactions).
3. **Integrity and Availability:** Ensure command and telemetry integrity and safe failover behavior under attacks.
4. **Privacy:** Protect raw biometric signals and derived templates; minimize data exfiltration risk.
5. **Auditability:** Provide verifiable logs for incident investigation and regulatory compliance.

## 5. Design Framework: Biometric-Enabled Robot Access Control (BERAC)

We propose BERAC, a layered architecture combining on-device biometrics, cryptographic attestation, context-aware access control, and fail-safe clinical policies. BERAC is designed for modular adoption by device vendors and hospital IT.

### 5.1. Architectural components

1. **Sensor & Enrollment Layer:** Multi-modal biometric sensors (fingerprint/IR/PPG/ECG/gait) with secure enrollment. Enrollment can be on-device with mutual attestation between device and identity provider.
2. **On-device Biometric Engine:** Runs template extraction and matching within a hardware-protected boundary (TPM/secure enclave). Matching thresholds are adaptive based on context (emergency vs. routine).
3. **Authenticator Broker & Key Management:** Issues short-lived attestations (cryptographic tokens) to authenticated users; keys are rotated and protected. Broker can be cloud-based or on-prem for sensitive environments.
4. **Policy Engine (ABAC):** Evaluates policies combining role, location, device state (battery, network health), patient consent, and biometric assurance level to produce fine-grained permissions.
5. **Command Control & Runtime Monitor:** Mediates all robot actuation commands, enforcing rate limiters, safety envelopes (physical constraints), and anomaly detection for telemetry and command patterns.
6. **Audit & Forensics Module:** Immutable logging (e.g., append-only ledger or secure logging) with tamper-evidence and retention policies for compliance (Fatunmbi, 2022).

A simplified data-flow: sensor → on-device match → broker attestation → policy evaluation → command execution (or deny), with continuous monitoring during session.

### 5.2. Multimodal fusion and adaptive assurance

BERAC uses **graded assurance**: stronger cryptographic attestations and stricter command privileges require higher biometric assurance (e.g., match score + continuous confirmation). In emergencies, a predefined override policy allows constrained actuation with mandatory post-event auditing to balance safety and security.

### 5.3. Template protection and privacy-preserving methods

To protect biometric data, BERAC implements cancellable templates, secure sketches, and where possible, on-device homomorphic matching or secure enclaves so raw signals never leave the device. When cloud processing is required, encrypted feature representations and tokenization reduce privacy risk.

## 6. Implementation Considerations

### 6.1. Hardware and real-time constraints

Robots often run on embedded platforms with limited CPU and power budgets. Implementations should use optimized matching algorithms, hardware acceleration for crypto, and lightweight anomaly detectors. Choice of biometric sensor must account for typical clinical constraints (e.g., gloved hands, mask usage) and be validated in-situ.

### 6.2. Network and latency management

Authentication and policy evaluation may be hybrid (on-device + cloud). BERAC prescribes local enforcement for safety-critical actuation to avoid dependence on unreliable networks, with periodic reconciliation to central logs. Latency budgets for authentication flows must be established to avoid disrupting clinical workflows.

### 6.3. Human factors and clinical workflow integration

Design must minimize interruptions and false rejections; user studies indicate moderate willingness among clinicians to adopt robots, contingent on perceived safety and usability—thus usability testing is fundamental. Emergency workflows must be co-designed with clinicians to define override semantics and audit backstops.

### 6.4. Lifecycle management & patching

FDA guidance emphasizes secure update mechanisms and monitoring for vulnerabilities. Device manufacturers must document vulnerability management, update strategies, and incident response plans as part of premarket submissions and postmarket surveillance.

## 7. Evaluation Plan

### 7.1. Datasets and benchmarks

Evaluation requires datasets representing clinical conditions (noise, PPE, stress), multimodal biometric samples, and simulated attack vectors (spoofing, replay, network manipulation). Where realistic patient data are used, IRB oversight and privacy safeguards are mandatory. Existing public datasets for PPG/ECG and face-with-mask can seed evaluation; device-specific data collection will be needed.

### 7.2. Metrics

- **Authentication:** False match rate (FMR), false non-match rate (FNMR), time-to-authenticate, liveness/spoof detection EER.
- **Access control:** Incorrect authorization (allow/deny) counts, policy decision latency.
- **Safety:** Task success rate, time-to-fallback, rate of safety violations under simulated adversary.
- **Privacy:** Degree of template leakage under threat models (quantified via reconstruction attacks).
- **Usability:** SUS scores, clinician interruption frequency, acceptance rates.

### 7.3. Adversarial testing

Simulate network-level attacks, insider misuse, and biometric spoofing (replay, synthetic signals) to evaluate robustness and detection. Red-team exercises should be timed and logged for continuous improvement.

## 8. Case Study: Medication-Delivery Robot Use Case (Design Walkthrough)

We sketch an instantiation of BERAC for a medication-delivery robot:

1. **Enrollment:** Pharmacists and nurses enroll fingerprints and PPG templates on an on-prem identity broker; device-bound keys are generated and attested.
2. **Routine ops:** Nurse authenticates via fingerprint + continuous PPG while near robot; broker issues ephemeral signed token with authorization scope (deliver medications to Ward A). Policy engine ensures medication type allowed and robot battery/state safe.
3. **Emergency override:** If biometric systems fail in an emergency, an emergency-cached policy allows limited manual control for 10 minutes with post-event audit and supervisor notification.
4. **Attack detection:** If telemetry indicates abnormal command sequences or network anomalies, robot switches to safe-halt and alerts SOC.

This case highlights practical trade-offs: emergency access vs. auditability, user convenience vs. assurance, and the need for in-hospital governance.

## 9. Privacy, Ethics, and Fairness

Biometric systems may exhibit demographic bias and raise surveillance concerns. BERAC recommends: (1) audit datasets and models for fairness, (2) prefer on-device matching to avoid centralized biometric repositories, (3) implement opt-in and narrow-use consent models for patient-related biometrics, and (4) use cancellable biometrics and template protection to allow revocation when needed. Human-centered design and transparency are necessary for acceptance.

## 10. Regulatory, Standards, and Compliance Alignment

Design choices should map to NIST's identity assurance levels (IAL/AAL) and the FDA's premarket cybersecurity recommendations. Manufacturers must maintain traceable cybersecurity risk management, software bill-of-materials (SBOM), and documented update/patch plans in line with recent FDA guidance. Hospitals should integrate BERAC policies into their IAM and SOC processes.

## 11. Limitations and Open Research Questions

- **Heterogeneity of devices:** Standardized APIs and interoperability for biometric modules are lacking.
- **Data scarcity:** High-quality, labeled multimodal datasets in real clinical settings are limited.
- **Bias and explainability:** More work needed to make biometric decisions explainable and audit-ready.
- **Lightweight secure computation:** On-device privacy-preserving matching under resource constraints remains an active area.
- **Human-robot trust dynamics:** Longitudinal studies on clinician trust and compliance under security constraints are sparse.

## 12. Conclusion

Integrating biometric authentication with context-aware robot access control offers a promising path to secure, usable healthcare robotics. BERAC synthesizes best practices—on-device biometric matching, cryptographic attestation, attribute-based policies, and continuous monitoring—while explicitly addressing privacy, emergency workflows, and regulatory alignment. Future work must validate BERAC in diverse clinical environments, expand datasets, and refine fairness and privacy-preserving techniques.

## References

1. Cruz, E. M. G. N. V., et al. (2024). Robotics Applications in the Hospital Domain: A Literature Review. *Proceedings/MDPI Robotics*, 7(6), 125. https://doi.org/10.3390/robotics7060125.
2. Doherty, C., et al. (2025). Privacy in consumer wearable technologies: a living review. *NPJ Digital Medicine*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12167361/.
3. El-Gazar, H. E., et al. (2024). Are nurses and patients willing to work with service robots in hospital settings? *BMC Nursing*, 23, Article 336. https://doi.org/10.1186/s12912-024-02336-7.

4. FDA. (2023). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* (Final Guidance). U.S. Food and Drug Administration. https://www.fda.gov/media/173516/download.

5. Gallo, G. D., et al. (2025). Internet of Medical Things Systems Review: Insights into Architectures and Security. *Sensors*, 25(9), 2795. https://doi.org/10.3390/s25092795.

6. Messinis, S., et al. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A systematic review. *Computer Networks*, Article. https://doi.org/10.1016/j.comnet.2024.108xxx.

7. Nigam, D., et al. (2022). Biometric Authentication for Intelligent and Privacy-Preserving Hospital Environments. *Sensors* (MDPI). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8970854/.

8. Ozcelik, M. M., et al. (2025). A Survey on Internet of Medical Things (IoMT): Enabling Technologies and Security. *Expert Systems*, Article. https://doi.org/10.1111/exsy.70010.

9. Suleski, T., et al. (2023). A Data Taxonomy for Adaptive Multifactor Authentication in Healthcare. *JMIR Medical Informatics*, 11, e44114. https://www.jmir.org/2023/1/e44114/.

10. Wang, R., et al. (2023). A Medical Assistive Robot for Telehealth Care During the COVID-19 Pandemic. *JMIR Human Factors*, Article e42870. https://humanfactors.jmir.org/2023/1/e42870/.

11. Yadav, S., et al. (2024). Transformative Frontiers: A Comprehensive Review of VR/AR and IoMT. *Frontiers/PMC*, Article. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11027446/.

12. Zhang, B., et al. (2025). A survey on security and privacy issues in wearable health devices. *Computers & Security*. https://doi.org/10.1016/j.cose.2025.102xxx.

13. [International guidance] National Institute of Standards and Technology. (2025). *NIST Special Publication 800-63-4: Digital Identity Guidelines*. NIST. https://pages.nist.gov/800-63-4/.

14. [FDA policy summary] U.S. Food & Drug Administration. (2023). Cybersecurity (Digital Health Center of Excellence). https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

15. Fatunmbi, T. O. (2022). Leveraging robotics, artificial intelligence, and machine learning for enhanced disease diagnosis and treatment: Advanced integrative approaches for precision medicine. *World Journal of Advanced Engineering Technology and Sciences*, 6(2), 121-135. https://doi.org/10.30574/wjaets.2022.6.2.0057.

16. Fatunmbi, T. O. (2024). Predicting precision-based treatment plans using artificial intelligence and machine learning in complex medical scenarios. *World Journal of Advanced Engineering Technology and Sciences*, 13(1), 1069–1088. https://doi.org/10.30574/wjaets.2024.13.1.0438.

17. Adeyemo, A., et al. (2025). Utilisation of robots in nursing practice: an umbrella review. *BMC Nursing / PMC*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11881500/

18. Elikhchi, H. D., & Hamid, T. (2025). Cybersecurity in Robotic Healthcare Systems: A Critical Thematic Review. *International Journal of Computer Applications*, 187(32), 65–79.

19. Suleski, T. (2023). A review of multi-factor and adaptive authentication in healthcare. *ECUworks/Conference Proceedings*.