Zero Trust Access Policy for ERM Systems

Table of Contents

1. Purpose
2. Scope
3. Access and Authentication Controls
4. Device Security Requirements
5. Role-Based Access Control (RBAC)
6. Monitoring and Auditing
7. Incident Response
8. Compliance and Enforcement
9. References
10. Document Control

Policy Content

1. Purpose

This policy establishes a Zero Trust security framework for accessing Emergency Medical Records (ERM) systems. It ensures that patient data access is tightly controlled, continuously monitored, and compliant with HIPAA, NIST SP 800-207, and ISO/IEC 27001.

2. Scope

Applies to:

* Hospital staff, contractors, and authorized third parties accessing ERM.
* Hospital-issued devices and mobile endpoints.
* Administrative systems and privileged accounts.
* Sensitive patient data, including narcotics and VIP patient records.

3. Access and Authentication Controls

* MFA Required: Every user must authenticate using multi-factor authentication.
* Least Privilege: Users only access what is necessary for their role.
* Privileged Accounts: Must be logged, monitored, and reviewed periodically.
* Sensitive Data Verification: Access to narcotics or VIP records requires additional authorization.

4. Device Security Requirements

* Only hospital-issued devices allowed.
* Devices must use a segregated, encrypted network.
* Devices must have endpoint protection, encryption, certificates, and regular patching.
* Compromised devices must be removed for repair.

5. Role-Based Access Control (RBAC)

* Access depends on role.
* VIP/high-value floors require extra verification.
* Emergency access protocols (“break-glass”) must exist, and all activity logged.

6. Monitoring and Auditing

* All access is logged and monitored.
* Security events reviewed regularly.
* Continuous monitoring of privileged accounts required.

7. Incident Response

* Incident response procedures must exist.
* Staff must report anomalies immediately.
* Emergency access events are reviewed post-incident.

8. Compliance and Enforcement

* Security team enforces this policy.
* Noncompliance triggers corrective measures.
* Policy reviewed annually or when regulations change.

9. References

* NIST SP 800-207 – Zero Trust Architecture
* HIPAA Security Rule (45 CFR Part 164)
* ISO/IEC 27001:2022 – Information Security Management
* ISO/IEC 27002:2022 – Information Security Controls

10. Document Control

| Version | Date | Author | Description | Approved By |
| --- | --- | --- | --- | --- |
| 1.0 | 10/14/2025 | Keitavius Alexadner | Initial Draft | KA |