# MEDAIPRO HIPAA Compliance Policy

***Last Updated: August 04, 2025 | Version 1.0***

**Our Commitment to Protecting Patient Health Information**

At MEDAIPRO, HIPAA compliance is more than a legal requirement—it's a core responsibility. Our EMR platform is designed to meet and exceed HIPAA standards (45 CFR Parts 160, 162, and 164), HITECH Act requirements, and state privacy laws. Through rigorous annual audits, we maintain compliance to ensure the highest data protection standards for your practice and patients.

**Administrative Safeguards**

- **Risk Management:** Annual NIST-based risk assessments with quarterly reviews
- **Workforce Training:** Mandatory HIPAA training with bi-annual refreshers
- **Policies & Procedures:** Comprehensive PHI handling documentation
- **Vendor Management:** Strict vetting with enforceable BAAs for all partners

**Physical Safeguards**

- **Infrastructure Security:**
  - • SOC 2 Type II-certified AWS data centers
  - • 24/7 monitoring with biometric access
  - • Environmental protections (fire suppression, climate control)
- **Device Protection:**
  - • Full-disk encryption on all devices

• Mobile Device Management (MDM) enforcement

• Secure disposal per NIST 800-88 guidelines

**Technical Safeguards**

- **Access Controls:**

  • Mandatory multi-factor authentication (MFA)

  • Unique user identification

  • Automatic session termination after 15 minutes

- **Encryption:**

  • AES-256 for data at rest

  • TLS 1.3+ for data in transit

  • End-to-end encrypted messaging

- **Audit Systems:**

  • Immutable PHI access logs

  • 6-year retention period

  • Real-time anomaly detection

**SureScripts-Specific Compliance**

1. **e-Prescribing Protection:**
    - Industry-standard protocols
    - Two-factor authentication for controlled substances
    - Real-time prescription drug monitoring (PDMP)
2. **Secure Medical Records Sharing:**
    - Encrypted Direct Messaging

    - Protected API integrations
    - Automated CCD-A generation
3. **Pharmacy Integration:**
    - Real-time medication history updates
    - Benefit coverage insights
    - Refill status alerts\

**Business Associate Agreements (BAAs)**

- Explicit PHI handling requirements
- Mandatory security incident notifications
- Subcontractor compliance verification
- Defined audit rights and breach liabilities

**Patient Rights Management**

- **Access**: Secure portal for record requests
- **Amendments**: Electronic request processing
- **Disclosures**: Automated accounting reports
- **Restrictions**: Granular consent controls

**Incident Response & Breach Protocol**

1. Immediate system containment
2. Forensic investigation launch
3. Breach scope determination
4. Notification initiation (within 24 hours)

5. Regulatory coordination
6. Remediation implementation
7. Process review and improvement

***Breach Notifications*:**

- **Affected individuals within 60 days**
- **HHS reporting for 500+ affected**
- **Media notifications when required**

**Compliance Validation**

- HITRUST CSF Certified
- SureScripts Certified Partner
- Annual audits by KirkpatrickPrice
- Quarterly penetration testing
- Continuous monitoring:
    - SIEM threat detection
    - Weekly vulnerability scans
    - Automated Vanta compliance checks

**Contact & Policy Management**

- **Compliance Inquiries:**

  **compliance@medaipro.com | (800) 555-HEALTH**

- **Security Emergencies:**

  **security@medaipro.com | 24/7 Hotline: (800) 555-SECURE**
- **SureScripts Support:**

  **surescripts@medaipro.com | (800) 555-SCRIPT**

**Corporate Office:**

MEDAIPRO Compliance Department

123 Healthcare Boulevard

Boston, MA 02110

***Policy Management*:**

- Last Reviewed: August 04, 2025 by Dr. Viola Jacob
- Next Scheduled Review: February 04, 2026