MERCIFUL O&P
FAMILY ORTHOTICS AND PROSTHETIC SERVICES

HIPAA Security Policy

Merciful O&P
Effective Date: 3/1/2025

---

1. Purpose *(ABC Standard: Information Security / HIPAA Security Rule)*
The purpose of this HIPAA Security Policy is to establish safeguards to protect electronic Protected Health Information (ePHI) in compliance with the HIPAA Security Rule, HITECH Act, and ABC Accreditation Standards. Merciful O&P is committed to ensuring the confidentiality, integrity, and availability of ePHI.

---

2. Scope *(ABC Standard: Policy Applicability)*
This policy applies to all workforce members, contractors, volunteers, information systems, and devices that create, access, transmit, or store ePHI on behalf of Merciful O&P.

---

3. Definitions *(ABC Standard: HIPAA Terminology)*
- ePHI: Electronic Protected Health Information
- Workforce: Employees, contractors, students, and volunteers
- Information Systems: Hardware, software, networks, and electronic media

---

4. Administrative Safeguards *(ABC Standard: Administrative Controls)*
4.1 Security Management Process
Merciful O&P implements administrative controls to prevent, detect, contain, and correct security violations, including:
- Risk analysis and periodic risk assessments
- Risk management and mitigation planning
- Sanction policies for workforce noncompliance
- Regular review of system activity and access logs

4.2 Assigned Security Responsibility
A designated Security Officer is responsible for overseeing HIPAA security compliance and implementation.
Security Officer Contact:
Name/Title:
Staci MacKay -Owner
770-800-2030 staci@mercifuloandp.com
4.3 Workforce Security
- Access to ePHI is granted based on job role and minimum necessary principles
- Workforce access is terminated promptly upon separation

4.4 Workforce Training and Awareness
All workforce members receive HIPAA Security training upon hire and periodically thereafter, including training on password management, phishing awareness, and device security.

---

5. Physical Safeguards *(ABC Standard: Physical Security Controls)*
5.1 Facility Access Controls
- Access to areas containing ePHI is restricted to authorized personnel
- Doors, file rooms, and server locations are secured

5.2 Workstation Use and Security
- Workstations are positioned to prevent unauthorized viewing of ePHI
- Automatic screen locks are enabled
- Workforce members log out when systems are unattended

5.3 Device and Media Controls

- Inventory and control of devices containing ePHI
- Secure disposal or destruction of electronic media
- Data is removed prior to device reuse or reassignment

---

6. Technical Safeguards *(ABC Standard: Technical Controls)*

6.1 Access Control

- Unique user IDs for system access
- Strong password requirements and authentication controls
- Role-based access permissions

6.2 Audit Controls

Merciful O&P maintains audit controls to record and examine system activity involving ePHI.

6.3 Integrity Controls

Technical measures are implemented to protect ePHI from improper alteration or destruction.

6.4 Transmission Security

- ePHI transmitted electronically is protected through encryption or secure transmission methods
- Public or unsecured networks are avoided when transmitting ePHI

---

7. Incident Response and Breach Management *(ABC Standard: Incident Reporting & Response)*

Merciful O&P maintains procedures for identifying, responding to, mitigating, and documenting security incidents involving ePHI. Breaches are assessed and reported in accordance with HIPAA and ABC requirements.

---

8. Business Associate Security *(ABC Standard: Vendor Oversight)*

All Business Associates with access to ePHI must sign a Business Associate Agreement (BAA) and demonstrate compliance with HIPAA Security Rule requirements.

---

9. Evaluation *(ABC Standard: Ongoing Compliance Monitoring)*

Merciful O&P conducts periodic technical and non-technical evaluations to ensure continued compliance with HIPAA Security standards and to address changes in technology or operations.

---

10. Policy Enforcement *(ABC Standard: Sanctions & Accountability)*

Failure to comply with this policy may result in disciplinary action, up to and including termination, and possible legal consequences.

---

11. Policy Maintenance *(ABC Standard: Documentation & Review)*

This HIPAA Security Policy is reviewed periodically and updated as necessary to remain compliant with regulatory and accreditation requirements.