

HIPAA SECURITY RULE COMPLIANCE ASSESSMENT

DeepShield Systems, Inc.

Assessment Date: January 11, 2024

Reference: DSS-HIPAA-2024-001

1. EXECUTIVE SUMMARY

This HIPAA Security Rule Compliance Assessment evaluates DeepShield Systems, Inc.'s ("DeepShield") compliance with the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as it relates to the company's industrial cybersecurity solutions deployed in healthcare environments.

2. SCOPE OF ASSESSMENT

1. This assessment covers DeepShield's integrated industrial cybersecurity platform and associated services when implemented within healthcare facilities or handling electronic Protected Health Information ("ePHI").
2. Assessment period: January 1, 2023 - December 31, 2023
3. Facilities reviewed: Delaware headquarters and three regional operations centers
4. Systems evaluated: DeepShield ICS Security Platform v4.2, OT Network Monitor v3.1, Threat Detection Module v2.8

3. ADMINISTRATIVE SAFEGUARDS ASSESSMENT

1. Security Management Process

- Comprehensive risk analysis conducted quarterly
- Documented risk management procedures in place
- Regular sanction policies for security violations
- System activity review procedures implemented

2. Assigned Security Responsibility

- Chief Security Officer: Dr. Elena Rodriguez
- HIPAA Security Officer: Michael Thompson

- Documentation of delegation of authority maintained

3. Workforce Security

- Authorization and supervision procedures established
- Workforce clearance procedures documented
- Termination procedures aligned with HIPAA requirements

4. Information Access Management

- Access authorization protocols implemented
- Access establishment workflows documented
- Access modification procedures maintained

4. PHYSICAL SAFEGUARDS ASSESSMENT

1. Facility Access Controls

- Facility security plan implemented
- Access control and validation procedures in place
- Maintenance records documented
- Workstation security protocols established

2. Workstation and Device Security

- Workstation use policies documented
- Device and media controls implemented
- Hardware inventory maintained
- Mobile device management protocols in place

5. TECHNICAL SAFEGUARDS ASSESSMENT

1. Access Control

- Unique user identification implemented
- Emergency access procedure established
- Automatic logoff configured
- Encryption and decryption capabilities verified

2. Audit Controls

- System activity logging enabled
- Audit trail implementation verified
- Review procedures documented

3. Integrity Controls

- Authentication mechanisms implemented
- Electronic mechanism to corroborate ePHI maintained
- Error correction procedures documented

4. Transmission Security

- Integrity controls during transmission verified
- Encryption protocols implemented
- Secure transmission channels established

6. BUSINESS ASSOCIATE AGREEMENTS

1. DeepShield maintains appropriate Business Associate Agreements with:

- Healthcare facility clients
- Third-party service providers
- Cloud infrastructure providers
- Managed security service partners

7. FINDINGS AND RECOMMENDATIONS

1. Areas of Compliance

- Administrative safeguards fully implemented
- Physical security controls meet requirements
- Technical safeguards exceed minimum standards
- Documentation procedures properly maintained

2. Areas Requiring Attention

- Enhanced audit logging for OT systems recommended
- Additional encryption protocols for legacy systems needed
- Updated incident response procedures required

- Additional staff training recommended

8. CERTIFICATION

Based on our assessment, DeepShield Systems, Inc. demonstrates substantial compliance with HIPAA Security Rule requirements. Minor remediation items identified in Section 7.2 should be addressed within 90 days.

9. ATTESTATION

This assessment was conducted in accordance with industry standards and regulatory requirements by qualified security professionals.

Prepared by:

/s/ Jennifer Martinez, CISSP, HCISPP

Lead Security Auditor

DeepShield Systems, Inc.

Reviewed by:

/s/ Michael Thompson

HIPAA Security Officer

DeepShield Systems, Inc.

Approved by:

/s/ Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 11, 2024

10. LEGAL DISCLAIMER

This assessment represents a point-in-time evaluation of security controls and compliance measures.

It should not be construed as a guarantee of ongoing compliance or security effectiveness.

DeepShield Systems, Inc. assumes no liability for subsequent security incidents or compliance violations that may occur after the assessment date.