

ALCOHOL, DRUG ADDICTION AND MENTAL HEALTH SERVICES BOARD OF CUYAHOGA COUNTY

POLICY STATEMENT

SUBJECT: SECURITY OF CLIENT INFORMATION - ADMINISTRATIVE SAFEGUARDS

EFFECTIVE DATE: May 27, 2026

PURPOSE

The purpose of this policy is to define the ADAMHS Board's Administrative Safeguards for protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI) that the Board creates, receives, maintains, or transmits. These safeguards ensure compliance with the Administrative Requirements of the HIPAA Security Rule (45 CFR Part 164 Subpart C) and establish organizational practices necessary to manage security risks across all systems, services, and workforce members.

POLICY STATEMENT

The Administrative Safeguards described herein are intended to: (i) ensure the confidentiality, integrity, and availability of ePHI across all environments in which it is accessed or stored, including cloud-based systems and Board-managed devices; (ii) protect against reasonably anticipated threats, vulnerabilities, or hazards to the security or integrity of ePHI; (iii) protect against any reasonably anticipated uses or disclosures of ePHI not permitted or required by HIPAA (see Policy on Privacy and Confidentiality of Client Information); and (iv) ensure workforce compliance with all security requirements through defined roles, responsibilities, training, and enforcement processes.

A. SECURITY MANAGEMENT PROCESS

Risk Analysis

The Board conducts periodic assessments of potential risks and vulnerabilities to ePHI. Risk analyses are performed at least once every year, when significant changes occur to technology, systems, or physical safeguards, or in response to environmental or operational changes affecting ePHI security.

The Security Officer is responsible for ensuring that risk analyses identify and document the scope of ePHI, systems, processes, and storage locations; assess potential threats and vulnerabilities; evaluate existing security controls; and recommend measures to reduce risk to a reasonable and appropriate level. External contractors or vendors may assist with risk analyses as needed. All risk analysis documentation is retained in accordance with the Records Retention Policy.

Reference: 45 CFR 164.308(a)(1)(ii)(A) | NIST SP 800-30 | CIS Control 18

Risk Management

The Board implements security measures to reduce identified risks and vulnerabilities to a reasonable and appropriate level. The Security Officer, in conjunction with Executive Leadership, oversees a Risk Management Plan that defines required safeguards, ensures the confidentiality, integrity, and availability of ePHI, protects against anticipated threats or unauthorized disclosures, and measures compliance through periodic evaluation of security controls.

Decisions to defer any recommended security control must be documented and approved by the Security Officer and Chief Executive Officer. All risk management documentation is retained in accordance with the Records Retention Policy.

Reference: 45 CFR 164.308(a)(1)(ii)(B) | NIST SP 800-30 | CIS Control 18

Information System Activity Review

The Board monitors and reviews activity on systems containing ePHI to detect unauthorized access or anomalous behavior. Because all Board systems, services, and storage environments are treated as potentially containing ePHI, the Security Officer and/or designee shall maintain an inventory of all Board systems and shall oversee activity monitoring across all environments accordingly.

The Security Officer conducts an internal audit log review annually. Findings are documented and acted upon in accordance with the Incident Response Plan. Notifications of security incidents are sent to appropriate personnel including the Security Officer and Executive Leadership.

Reference: 45 CFR 164.308(a)(1)(ii)(D) | CIS Controls 8, 13

B. ASSIGNED SECURITY RESPONSIBILITY

Security Officer

The Board designates the Director of IT as the Security Officer. This role is responsible for developing, implementing, and maintaining the Board's security policies and procedures to protect ePHI. The Security Officer is responsible for:

- Overseeing the Board's information security program including administrative, technical, and physical safeguards.
- Ensuring compliance with the HIPAA Security Rule (45 CFR Part 164 Subpart C).
- Coordinating risk analyses, risk management, workforce training, and security incident response.
- Monitoring system activity, access controls, and audit processes.
- Ensuring timely updates to policies, controls, and documentation.
- Collaborating with Executive Leadership, Human Resources, and other departments as needed.

HIPAA Privacy Officer

The Board designates the Chief of External Affairs as the HIPAA Privacy Officer. This role is distinct from the Security Officer and is responsible for developing and implementing privacy policies and procedures, ensuring workforce compliance with HIPAA Privacy Rule requirements and 42 CFR Part 2, overseeing the handling of privacy-related complaints, and coordinating breach notification procedures in accordance with the Board's Policy on Privacy and Confidentiality of Client Information.

The names and roles of both the Security Officer and Privacy Officer will be communicated to all Board workforce members and included in their respective position descriptions.

Reference: 45 CFR 164.308(a)(2) | CIS Control 17

C. WORKFORCE SECURITY

Authorization, Supervision, and Clearance

The Board implements procedures to ensure that workforce access to ePHI is appropriate to each member's role.

The background of all Board workforce members must be adequately reviewed during the hiring process by the Chief Human Resources Officer so that a determination of trustworthiness can be made before allowing access to sensitive information. Proper background checks include confirmation of academic and professional qualifications, professional license validation, criminal background check (BCI), and character references. When a workforce member is provided by an employment agency, the Chief Human Resources Officer will determine whether the agency's screening process is adequate or whether additional checks are necessary.

All workforce members must sign a statement acknowledging their commitment to and understanding of their responsibility for the protection of the confidentiality, integrity, and availability of ePHI.

Access to systems and information containing ePHI is granted based on a workforce member's job role and documented in the Board's access inventory, consistent with the Requesting IT Equipment and Access Policy. Supervisors are responsible for identifying the level of access required for their staff. The IT Department is responsible for implementing, managing, and enforcing approved access permissions. Requests for access beyond standard role-based permissions must be explicitly approved and documented. All access permissions are subject to periodic review.

A workforce member who is promoted or transferred with substantially greater responsibility for or access to ePHI shall receive appropriate training prior to that access being granted.

Reference: 45 CFR 164.308(a)(3)(ii)(A) and (B) | CIS Controls 5, 6

Workforce Termination

The Board implements procedures to ensure timely removal or modification of access to ePHI when a workforce member separates from employment, changes roles, or when a Business Associate relationship ends.

The Chief Human Resources Officer shall notify the Security Officer when workforce access to ePHI is no longer appropriate. The Security Officer, in coordination with the IT Department, shall ensure access is removed or modified in accordance with established procedures, including preventing authentication to Board systems, revoking or modifying logical and physical access, and ensuring continuity of business operations and preservation of Board data.

When a workforce member's job duties change, access associated with prior duties shall be removed and new access granted based on role-based access controls and documented authorization. All termination and access modification actions shall be documented and retained in accordance with the Records Retention Policy. Executive Leadership, along with the IT Department, will collect all Board assets and coordinate their redistribution.

Reference: 45 CFR 164.308(a)(3)(ii)(C) | CIS Controls 5, 6

D. INFORMATION ACCESS MANAGEMENT

Access to ePHI shall be authorized, established, documented, reviewed, and modified in a manner that supports the Board's operational needs and complies with HIPAA requirements.

The minimum necessary standard governs all access decisions at the Board. Workforce members and contractors shall be granted access only to the ePHI and systems required to perform their specific job functions. Access shall not be granted beyond what is operationally necessary, and all access permissions shall be reviewed periodically to ensure continued alignment with current job responsibilities.

Access shall be granted based on a workforce member's or contractor's job role, assigned duties, and the minimum necessary standard, as defined by position descriptions, role-based access controls, and the Board's documented access inventory. Supervisors or designated Executive Staff are responsible for initiating access requests. The IT Department, under the direction of the Security Officer, shall establish access in accordance with approved requests and applicable security policies, consistent with the Requesting IT Equipment and Access Policy.

Access shall be reviewed and modified when a workforce member's or contractor's role, duties, or relationship with the Board changes. All access authorization, modification, and termination actions shall be documented and retained for compliance and audit purposes.

Reference: 45 CFR 164.308(a)(4)(ii)(B) and (C) | CIS Controls 5, 6

E. SECURITY AWARENESS AND TRAINING

Security Training Program

The Security Officer shall oversee the Board's security training program. Training shall be provided to all workforce members and shall address the appropriate use, access, and security of ePHI. Training content shall ensure workforce members understand their responsibilities under HIPAA, 42 CFR Part 2,

and the Board's security policies. Detailed training content, delivery methods, schedules, and tracking requirements are governed by the Cybersecurity Training and Awareness Plan.

Training shall be provided as follows:

- a. General security awareness or targeted training to new workforce members within 90 days of employment.
- b. Quarterly security awareness training to all workforce members.
- c. Specific security training to affected workforce members within 60 days of environmental or operational changes that affect the security of ePHI.
- d. Annual mandatory training to all workforce members, led by the Security Officer, covering HIPAA requirements and 42 CFR Part 2, with emphasis on the privacy and security of protected health information.

The Security Officer shall retain records of each training provided, including sign-in sheets and copies of training materials, in accordance with the Records Retention Policy.

Reference: 45 CFR 164.308(a)(5)(i) | CIS Control 14

Security Reminders

The Security Officer, in coordination with the IT Department, is responsible for maintaining awareness of emerging threats and distributing periodic notices and reminders to the workforce regarding Board security policies and legal requirements, changes to security policies and procedures, discovered or reported threats or vulnerabilities affecting ePHI, emerging risks including the prohibited use of generative AI tools and large language models that have not been approved for handling ePHI, and best security practices for specific staff or departments.

Reminders will be distributed via email, postings in common areas, and staff meetings as appropriate. Provision of security reminders shall be documented to include the type of reminder, summary of message, and date.

Reference: 45 CFR 164.308(a)(5)(ii)(A) | CIS Control 14

Protection from Malicious Software

The Security Officer, in coordination with the IT Department, shall implement and maintain administrative, technical, and physical safeguards to protect Board systems from malicious software. These safeguards include centrally managed endpoint protection, network security controls, application restrictions, and timely system updates. Security controls for cloud-hosted systems shall be maintained by contracted service providers in accordance with applicable security standards and Board requirements. Detailed procedures are documented in the Incident Response Plan.

Workforce members must promptly report suspected or confirmed malicious or unauthorized software to the Security Officer. Upon identification of a potential threat, affected systems shall be isolated as necessary and workforce members must follow all instructions from IT personnel to contain and remediate the incident. The Security Officer shall ensure such incidents are documented and communicated to appropriate leadership. When required, notification to the Auditor of State shall be made by the Security Officer in accordance with applicable reporting requirements.

Reference: 45 CFR 164.308(a)(5)(ii)(B) | CIS Controls 7, 10

Log-In Monitoring

Authentication attempts to Board systems and cloud services are logged and monitored to identify suspicious or unauthorized activity through Microsoft Entra ID, Microsoft 365, and Microsoft Purview audit logging. Because all Board systems are treated as potentially containing ePHI, logging applies across all environments. Logs capture user identity, system or service accessed, source device or IP address, authentication outcome, and date and time of the event.

Suspicious or repeated failed authentication attempts, anomalous sign-in behavior, or indicators of potential compromise shall be reviewed and reported to the Security Officer for investigation in accordance with the Incident Response Plan. Authentication security is enforced through MFA,

Conditional Access policies, and automated risk-based controls through Microsoft's identity protection mechanisms.

Reference: 45 CFR 164.308(a)(5)(ii)(C) | 45 CFR 164.312(b) | CIS Controls 6, 8

Password Management

The Board's password and authentication standards are governed by the Password Policy. That policy establishes requirements for password creation and strength, Windows Hello for Business and device-based authentication, MFA requirements, credential protection, compromise response, and account maintenance, consistent with NIST SP 800-63B and current federal guidance.

Reference: 45 CFR 164.308(a)(5)(ii)(D) | 45 CFR 164.312(a) | CIS Control 5

F. SECURITY INCIDENT PROCEDURES

The Board maintains a structured incident response and reporting program to address security incidents that threaten the confidentiality, integrity, or availability of ePHI. Security incidents include any event that compromises or threatens to compromise Board information systems, including attempted or actual unauthorized access, disruption or denial of service, malware activity, hardware or software compromise, and breaches of ePHI or other non-public information.

All workforce members and contractors must report suspected or confirmed security events to the Security Officer promptly. The Security Officer and/or designee shall assess reported events, coordinate response activities, and initiate containment, remediation, recovery, and post-incident analysis. Detailed response procedures, escalation criteria, notification roles, documentation requirements, and external reporting obligations under Ohio Revised Code 9.64 are maintained in the Incident Response Plan.

The Security Officer or designee shall produce an annual security incident summary for review by the Executive Council. Records of security incidents and associated reports shall be retained in accordance with the Records Retention Policy.

Reference: 45 CFR 164.308(a)(6) | ORC 9.64 | CIS Controls 17, 18

G. CONTINGENCY PLAN

The Board maintains formal contingency planning processes to ensure the availability of ePHI and continuity of critical operations during and after an emergency or disruptive event.

Data Backup

Backup activities are performed in accordance with the Data Backup Policy and the Records Retention Policy.

Reference: 45 CFR 164.308(a)(7)(ii)(A)

Disaster Recovery and Emergency Operations

The Board maintains documented Disaster Recovery, Business Continuity, and COOP plans to support system recovery and continuation of essential functions. Detailed procedures and responsibilities are maintained in those internal planning documents.

Reference: 45 CFR 164.308(a)(7)(ii)(B) and (C)

Testing, Review, and Maintenance

Contingency-related plans are periodically reviewed and tested to ensure continued effectiveness, in accordance with internal procedures.

Reference: 45 CFR 164.308(a)(7)(ii)(D)

Application and Data Criticality

Information systems and data are evaluated based on sensitivity and operational criticality to ensure appropriate backup, recovery, and continuity controls are applied.

Reference: 45 CFR 164.308(a)(7)(ii)(E) | CIS Control 11

H. EVALUATION

The Board performs periodic technical and non-technical reviews to ensure ePHI is adequately protected. IT staff will review policies and procedures when new technology is implemented, when new risks, vulnerabilities, or infrastructure changes are identified, and at least every 24 months. All evaluations will be documented and retained in accordance with the Records Retention Policy. The Board may engage external experts when appropriate.

Reference: 45 CFR 164.308(a)(8) | CIS Control 18

I. BUSINESS ASSOCIATE AGREEMENTS

When entering into a Business Associate Agreement (BAA) or Memorandum of Understanding (MOU) with any entity that creates, receives, maintains, or transmits ePHI on behalf of the Board, the agreement must include assurances that the Business Associate will safeguard ePHI and report any security incidents including breaches as required by HIPAA, will comply with HIPAA Security Regulations, and will ensure that any subcontractors or downstream vendors handling ePHI also comply with HIPAA Security Regulations. Detailed BAA requirements and standard agreement templates are governed by the Business Associate Agreement SOP.

Critical vendors and Managed Service Providers (MSPs) that handle or have access to ePHI on behalf of the Board are subject to annual security review by the Security Officer. These reviews assess whether vendors maintain appropriate administrative, technical, and physical safeguards consistent with their contractual obligations and applicable HIPAA requirements. Findings from vendor reviews shall be documented and any identified deficiencies addressed in a timely manner.

Reference: 45 CFR 164.308(b), 164.314(a), 164.504(e)(2) | CIS Control 15

J. SANCTIONS

Appropriate sanctions shall be applied against workforce members who fail to comply with the Board's security policies and procedures, as required by the HIPAA Security Rule and applicable Ohio law. All workforce members and agents of the Board must adhere to these policies and all supervisors are responsible for enforcement.

Sanctions may range from counseling and written reprimand to suspension, termination, and referral to law enforcement or professional licensing authorities depending on the nature and severity of the violation. Violations may also constitute grounds for contract termination for Business Associates and contractors. Detailed violation levels and disciplinary guidelines are maintained in the Board's Sanctions and Disciplinary Procedures.

Any allegation of violation shall be reported to the Security Officer and/or Executive Leadership, who will conduct a confidential investigation. The Board will not retaliate against workforce members who report violations in good faith. In the event a breach of unsecured PHI is identified, breach notification procedures set forth in the Board's Policy on Privacy and Confidentiality of Client Information shall be followed.

Reference: 45 CFR 164.308(a)(1)(iii)(C) | ORC 1347.05

K. POLICIES, PROCEDURES, AND DOCUMENTATION

The Security Officer is responsible for providing security policies and procedures to workforce members responsible for implementation, periodically auditing compliance, reviewing policies annually and updating as needed based on environmental or operational changes, and documenting all changes and overseeing their implementation.

Security policies and procedures shall be maintained in written or electronic form. Written records shall be kept for all actions, activities, and assessments required by security policies and procedures. All documentation shall be retained in accordance with the Records Retention Policy.

Reference: 45 CFR 164.316 | CIS Control 18

RELATED POLICIES AND PROCEDURES

- HIPAA Security Regulations Compliance Policy
- Password Policy
- Remote Access Policy
- Mobile Device Policy
- Acceptable Use Policy
- IT Resource Usage and Security Policy
- Requesting IT Equipment and Access Policy
- Third-Party Account Creation Policy
- Data Backup Policy
- Data Handling and Classification Policy
- Cybersecurity Training and Awareness Plan
- Incident Response Plan
- Records Retention Policy
- Business Associate Agreement SOP
- Sanctions and Disciplinary Procedures
- Disaster Recovery Plan / Business Continuity Plan / COOP Annex

REFERENCES

- 45 CFR Part 164 Subpart C - HIPAA Security Rule Administrative Safeguards
- 42 CFR Part 2 - Confidentiality of Substance Use Disorder Patient Records
- ORC 9.64 - Cybersecurity Program and Incident Reporting Requirements
- ORC 1347.05 - Ohio Personal Information Systems Act
- CIS Critical Security Controls v8 - Controls 5, 6, 7, 8, 10, 11, 14, 15, 17, 18
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-53 Rev. 5 - Security and Privacy Controls
- NIST SP 800-63B - Digital Identity Guidelines
- ADAMHS Board Policy on Privacy and Confidentiality of Client Information

Signed by:

Patricia James-Stewart, M.Ed., LSW

AEEBCB3D8553442...

Patricia James-Stewart, M.Ed., LSW
Board Chairperson

5/27/2026

Approval Date

Signed by:

Jason Joyce

E44D00AF38EF407...

Jason Joyce
Chief Executive Officer

5/27/2029

Review Date