

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

## POLICY STATEMENT

**SUBJECT:** SECURITY OF CLIENT INFORMATION - TECHNICAL SAFEGUARDS  
**EFFECTIVE DATE:** May 27, 2026

---

### PURPOSE

---

The purpose of this policy is to describe the ADAMHS Board's Technical Safeguards for protecting the security of electronic protected health information (ePHI) that the Board creates, receives, maintains, or transmits, in compliance with the HIPAA Security Rule (45 CFR Part 164 Subpart C).

### POLICY STATEMENT

---

The Technical Safeguards described herein are intended to: (i) ensure the confidentiality, integrity, and availability of ePHI; (ii) protect against reasonably anticipated threats 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 applicable security requirements.

### A. ACCESS CONTROLS

---

The Board implements technical access controls to allow only authorized persons or software to access ePHI.

#### Unique User Identification

Each individual accessing the Board's information systems is assigned a unique user account to identify and track their activity. These accounts, combined with appropriate authentication methods, are used to monitor user activity within systems containing ePHI. Shared or generic accounts may only be used in approved cases, such as providing access to third-party resources, and must be documented and approved by the Security Officer.

#### Emergency Access

Contingency procedures for authorized users to obtain necessary ePHI during an emergency are set forth in the Board's Disaster Recovery Plan and Business Continuity Plan with COOP Annex.

#### Automatic Logoff

All workstations shall be configured to automatically log off users after fifteen (15) minutes of inactivity.

#### Encryption

All Board-issued desktops and laptops must have full-disk encryption enabled. Encryption keys for Azure-joined devices are securely stored in the user's Azure account, with an additional copy maintained in a separate secure cloud location to ensure recoverability. The encryption requirement applies to ePHI both at rest on Board-issued devices and in transit across all networks, with each addressed in the relevant sections of this policy.

*Reference: 45 CFR 164.312(a) | CIS Controls 3, 5, 6*

## B. AUDIT CONTROLS

---

The Board implements hardware, software, and procedural mechanisms to record and examine activity in systems containing ePHI.

- The Board utilizes Microsoft Purview Audit and other MSP monitoring tools to record and review user, system, and administrative activity across all information systems containing ePHI.
- The Security Officer, in coordination with the IT Department, is responsible for documenting and maintaining the audit mechanisms configured to meet compliance requirements.
- Audit logs are captured at the application, system, and user levels, focused on access to files and systems containing ePHI, including Microsoft 365 services such as SharePoint, OneDrive, Exchange Online, and Teams.
- At a minimum, audit logs will include user identity, login date and time, source, and resource or service accessed.
- Audit records will be retained in accordance with the Records Retention Policy.
- The Security Officer conducts an internal audit log review annually. Findings will be documented and acted upon in accordance with the Board's Incident Response Plan.
- In the event that the Board's ePHI inventory, information systems, or technology platforms change, audit mechanisms must be revised accordingly to ensure continued compliance.

*Reference: 45 CFR 164.312(b) | CIS Controls 8, 13*

## C. INTEGRITY CONTROLS

---

The Board implements policies and procedures to protect ePHI from improper alteration or destruction.

The Security Officer, working with the IT Department and MSPs, will identify, document, and implement integrity controls based on the results of the Board's risk analysis. These controls may include role-based access controls, version history and change tracking in Microsoft 365, file-level permissions and encryption, and automated backups managed through MSPs consistent with the Data Backup Policy.

Integrity controls shall be evaluated periodically to determine whether objectives are being met and whether revisions are necessary.

*Reference: 45 CFR 164.312(c) | CIS Controls 3, 10*

## D. AUTHENTICATION

---

The Board implements procedures to verify that persons or entities seeking access to ePHI are who they claim to be.

Users seeking access to any network, system, or application containing ePHI must verify their identity using a unique user account combined with secure authentication methods. Authentication is managed through Microsoft Entra ID and enforced across all Microsoft 365 and other Board-managed systems, including remote access endpoints. Authentication methods include passwords, multi-factor authentication (MFA), and single sign-on (SSO) where applicable.

No person or entity may misrepresent their identity by using another person's credentials to access Board systems or ePHI. No person shall share authentication credentials with anyone except when provided to IT staff for authorized support purposes. Workforce members engaging in misrepresentation shall be subject to sanctions as defined in the Administrative Safeguards Policy.

Detailed authentication standards, including password requirements, Windows Hello for Business configuration, and MFA requirements, are governed by the Password Policy.

*Reference: 45 CFR 164.312(d) | CIS Controls 5, 6*

## **E. TRANSMISSION SECURITY**

---

The Board implements technical security measures to guard against unauthorized access to ePHI transmitted over electronic communications networks.

### **Internal Network and Cloud Traffic**

The Board's internal network and cloud environments are secured through network segmentation, firewall protection, and encrypted communication protocols. All traffic within the local area network and between on-premises systems and cloud services such as Microsoft 365 and Azure is protected using TLS 1.2 or higher.

### **Remote Access**

Remote access to Board systems and ePHI is governed by the Remote Access Policy. All remote and cloud-based access is protected by MFA and Windows Hello for Business. Microsoft Conditional Access policies and encryption standards including TLS 1.2 and IPsec where applicable are enforced to safeguard ePHI during transmission. Access to ePHI stored in Microsoft 365 or Azure must occur through organization-managed devices or approved secure web portals.

### **Personal Device Use (BYOD)**

Personal devices may be used only for Microsoft Authenticator, Board email access, and phone communications. No ePHI may be downloaded, saved, copied, screenshotted, or stored locally on any personal device under any circumstances. Staff must not access ePHI through personal cloud accounts, personal storage applications, or any non-Board-managed platform, consistent with the Mobile Device Policy.

### **Third-Party Access**

Access to Board systems and ePHI by third parties is limited to MSPs and authorized contractors who require such access to perform Board-assigned duties, governed by the Third-Party Account Creation Policy. All such access must use encrypted communication protocols consistent with current NIST standards, including NIST SP 800-52 Rev. 2 and NIST SP 800-77 Rev. 1. All encryption technologies must be FIPS 140-3 validated. Access is limited to the minimum necessary and monitored by the IT Department and Security Officer.

### **Transmission of ePHI to External Entities**

All ePHI transmissions between the Board and external entities must occur through securely encrypted and authenticated channels, including encrypted email, secure file transfer (SFTP or HTTPS), or VPN connections meeting current NIST and FIPS 140-3 standards. Unencrypted transmission of ePHI is prohibited.

### **Email and Messaging**

ePHI may not be transmitted through unsecured or non-Board-approved email or messaging systems. Only Board-issued Microsoft 365 email accounts with encryption enabled may be used for transmitting ePHI, consistent with the IT Resource Usage and Security Policy.

### **Generative AI Tools and Large Language Models**

The input or transmission of ePHI into any generative AI tool, large language model, or AI-assisted platform is strictly prohibited unless the tool has been explicitly approved by the Security Officer and is governed by a signed Business Associate Agreement or equivalent data protection agreement ensuring the confidentiality and security of ePHI. Approved tools must operate within Board-managed environments with appropriate access controls. Unapproved consumer-facing AI platforms, regardless of perceived convenience or utility, do not meet this standard and must never be used to process, summarize, generate, or otherwise handle ePHI.

Additionally, workforce members shall not use any AI-generated content in client-facing or provider-facing communications without human review and verification for accuracy. The use of AI tools to draft

clinical, administrative, or legal communications does not remove the individual workforce member's responsibility for the accuracy and appropriateness of that content.

*Reference: 45 CFR 164.312(e) | CIS Controls 3, 12, 13 | NIST SP 800-52 Rev. 2, SP 800-77 Rev. 1 | FIPS 140-3*

## F. EQUIPMENT AND SYSTEM REQUIREMENTS FOR REMOTE ACCESS

---

IT Department staff shall ensure that all Board-issued equipment used for remote access complies with the following, consistent with the Remote Access Policy:

- Operating systems are current and up to date with the latest security patches.
- Endpoint Detection and Response (EDR) software is current and active.
- Adequate authentication, encryption, and firewall protections are in place.
- Automatic session termination after a period of inactivity is enabled.

*Reference: 45 CFR 164.312(a),(d),(e) | CIS Controls 4, 7*

## RELATED POLICIES AND PROCEDURES

---

- Password Policy
- Remote Access Policy
- Mobile Device Policy
- Third-Party Account Creation Policy
- IT Resource Usage and Security Policy
- Data Backup Policy
- Incident Response Plan
- Records Retention Policy
- Disaster Recovery Plan / Business Continuity Plan / COOP Annex

## REFERENCES

---

- 45 CFR 164.312 - Technical Safeguards (HIPAA Security Rule)
- 42 CFR Part 2 - Confidentiality of Substance Use Disorder Patient Records
- CIS Critical Security Controls v8 - Controls 3, 4, 5, 6, 7, 8, 10, 12, 13
- NIST SP 800-53 Rev. 5 - Security and Privacy Controls
- NIST SP 800-52 Rev. 2 - Guidelines for TLS Implementations
- NIST SP 800-77 Rev. 1 - Guide to IPsec VPNs
- NIST SP 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management
- FIPS 140-3 - Security Requirements for Cryptographic Modules
- 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