

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

POLICY STATEMENT

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

PURPOSE

The purpose of this policy is to describe the ADAMHS Board's Physical 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 Physical 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. CONTINGENCY OPERATIONS

The Board's Disaster Recovery Plan, Business Continuity Plan, and Continuity of Operations (COOP) Annex contain procedures to be followed during an emergency to allow facility access in support of data restoration and system recovery.

Reference: 45 CFR 164.310(a)(2)(i) | CIS Control 11

B. FACILITY ACCESS CONTROLS

The Board implements Facility Access Controls to: (1) safeguard its facilities and equipment from unauthorized physical access, tampering, and theft; (2) control and validate access based on role or function, including visitor, contractor, vendor, and consultant access; and (3) document repairs and modifications to physical components related to security.

Facility Security

The following procedures are implemented to safeguard the facility and equipment from unauthorized physical access, tampering, and theft:

- a. An armed physical security officer is posted at the entrance to the Board's offices.
- b. All Board employees must use their assigned computerized identification card to access the office.
- c. All visitors must check in and log their arrival and departure with the security officer. Visitors shall wear a visible badge at all times while on site. Access beyond the locked reception area requires authorized credentials or an employee escort. Contractors or vendors escorted to an approved work location may continue unaccompanied if prior authorization has been granted.
- d. Access to areas containing workstations with ePHI is restricted. Doors separating public areas from office spaces remain locked at all times.
- e. Unrecognized persons in areas containing ePHI will be asked about their authorization to be present.
- f. All hardware and related equipment is inventoried with asset tags.

- g. Local building codes will be observed. Doors to restricted areas, including the equipment room, remain locked at all times with access limited to authorized staff. Manufacturer recommendations on fire protection of individual hardware will be followed.

Access Control and Validation Procedures

The following access controls are implemented to prevent unauthorized access to ePHI:

- h. Employees shall not have access to workstations containing ePHI that are not in their respective departments.
- i. Visitors, contractors, staff, interns, and volunteers will not have access to areas with workstations containing ePHI unless required for authorized activities and accompanied by a Board employee.
- j. Workforce members shall inquire about the authorization status of persons when that information is not known to them.
- k. When a workforce member with access to substantial amounts of ePHI separates from employment, measures such as deactivating HID access cards and re-keying locks shall be implemented promptly, in coordination with IT access revocation procedures consistent with the Requesting IT Equipment and Access Policy.
- l. Access to software for testing and revision is limited to IT Department staff and authorized staff, vendors, consultants, and contractors.

Maintenance Records

A record shall be created and maintained for modifications to physical infrastructure components essential to ePHI security, including but not limited to lock changes, installation or removal of security devices, and door alterations.

- m. A maintenance record must be created for each such modification.
- n. Such repairs and modifications shall be documented and maintained by Executive Leadership or designee.
- o. All maintenance, managed service, and other agreements for hardware and software will be documented by the IT Department and reviewed on an annual basis.
- p. Maintenance records covered by this section must be securely stored.

Reference: 45 CFR 164.310(a) | CIS Controls 1, 11

C. WORKSTATION USE

Board-issued workstations, including office desktops and laptops deployed for remote work, are the property of the Board and are to be used for official Board business. Limited personal use is permitted during authorized break periods.

Workforce members are expected to understand their obligations to protect the security, confidentiality, and integrity of ePHI residing on Board workstations and associated networks. Detailed workstation use requirements, prohibited uses, and user security obligations are governed by the IT Resource Usage and Security Policy and the Acceptable Use Policy.

All workstations that access or contain ePHI shall be identified and inventoried. Staff using Board-issued devices for remote work are responsible for ensuring ePHI remains secure outside the office, including using secure locations, locking devices when unattended, and preventing unauthorized access, consistent with the Remote Access Policy.

Files containing ePHI shall not be moved to removable media or portable devices unless the workforce member has received written approval from the Security Officer.

Reference: 45 CFR 164.310(b) and (c) | CIS Controls 1, 4

D. DEVICE AND MEDIA CONTROLS

Accountability

1. All electronic devices with data storage capability shall be identified and inventoried with notations for assigned user, asset tag, and serial number. Inventories shall be retained in accordance with the Records Retention Policy.
2. The IT Department shall record the receipt, removal, and return of hardware containing ePHI.
3. No workforce member shall transfer ePHI to removable media or portable devices except IT Department staff or those authorized in writing by the Security Officer.
4. An exact retrievable copy of ePHI must be available prior to movement of equipment, media, or devices storing that ePHI.
5. No workforce member shall remotely access ePHI except through an authorized Board-issued device, unless the data was transmitted via encrypted email, consistent with the Remote Access Policy.
6. Any lost or stolen Board-issued device must be reported immediately to the IT Department. The IT Department maintains remote wipe capability for all Board-managed devices. Full-disk encryption on all Board devices ensures ePHI remains protected in the event of loss or theft.

Device and Media Re-Use

7. Prior to making storage devices or removable media available for reuse, IT Department staff shall ensure the device does not contain ePHI, or that ePHI has been securely removed using approved methods.
8. All storage media must be fully sanitized in accordance with NIST SP 800-88 (Guidelines for Media Sanitization) prior to reuse or reassignment, regardless of media type.

Data Backup and Storage

The Board's data, including ePHI, is primarily stored and backed up in secure cloud environments managed by approved Managed Service Providers (MSPs). Backup, restoration, and storage processes are administered in accordance with the Data Backup Policy.

Staff are prohibited from saving ePHI to local drives, removable media, or personal storage locations except as authorized and in accordance with Board policy.

Disposal and Secure Data Removal

IT Department staff shall ensure that devices and media are properly disposed of when no longer needed. Prior to disposal or reassignment, all storage media must be fully sanitized in accordance with NIST SP 800-88 prior to disposal, regardless of media type. Disposal may be performed using approved tools or through a licensed and certified vendor. Cloud-stored ePHI remains managed by approved MSPs in accordance with Board policies and the Disaster Recovery Plan.

Reference: 45 CFR 164.310(d) | CIS Controls 3, 10 | NIST SP 800-88

RELATED POLICIES AND PROCEDURES

- IT Resource Usage and Security Policy
- Acceptable Use Policy
- Remote Access Policy
- Mobile Device Policy
- Requesting IT Equipment and Access Policy
- Data Backup Policy
- Records Retention Policy
- Disaster Recovery Plan / Business Continuity Plan / COOP Annex
- Physical Security SOP

- Device Disposal and Media Sanitization SOP

REFERENCES

- 45 CFR 164.310 - Physical Safeguards (HIPAA Security Rule)
 - CIS Critical Security Controls v8 - Controls 1, 3, 4, 10, 11
 - NIST SP 800-53 Rev. 5 - Physical and Environmental Protection (PE), Media Protection (MP)
 - NIST SP 800-88 - Guidelines for Media Sanitization
 - 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

Signed by:

Jason Joyce

E44D00AF38EF407...

Jason Joyce
Chief Executive Officer

5/27/2026

Approval Date

5/27/2029

Review Date