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

POLICY STATEMENT

SUBJECT: SECURITY OF CLIENT INFORMATION – PHYSICAL SAFEGUARDS

EFFECTIVE DATE: MARCH 28, 2018

PURPOSE

The purpose of this policy is to describe the ADAMHS Board's Physical Safeguards for protecting the security of electronic personal health information (ePHI) that the ADAMHS Board creates, receives, maintains or transmits, in compliance with the Security Regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 CFR Part 164 Subpart C).

POLICY STATEMENT

The Physical Safeguards set forth below are intended to accomplish each of the following: (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 the HIPAA Privacy Regulations (*see Policy on Privacy and Confidentiality of Client Information)* and (iv) ensure compliance by the ADAMHS Board's workforce.

I. FACILITY ACCESS CONTROLS: To limit physical access to ePHI systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

A. Contingency Operations: The Board's *Disaster Recovery Plan and Emergency Mode Operations Plan* shall contain procedures that are to be followed in the event of an emergency to allow facility access in support of the restoration of lost data.

B. Facility Access Controls: The Board shall implement the following Facility Access Controls to: (1) safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft; (2) control and validate a person's access to facilities based on their role or function, including visitor, vendor or consultant access and access to software programs for testing and revision; and (3) document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

1. **Facility Security**

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

a. An armed physical security officer shall be posted at the entrance to the Board's offices for protection of its premises.
b. All Board employees must utilize the assigned computerized identification card to gain access to building.
c. All visitors must check in and log in and log out with the contracted physical security officer. Visitors shall wear visitor badges and be escorted by an employee at all times.
d. Access beyond the locked doors in the reception area requires authorized access or escort.
e. Access will be restricted to areas with workstations containing ePHI and doors will be locked at the close of each business day.
f. Unrecognized persons in areas containing ePHI will be asked about their authorization to be in that area.
g. All hardware and related equipment is inventoried with identification numbers.
h. Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

2. **Access Control and Validation Procedures**

The following access controls and validation procedures shall be implemented to prevent unauthorized access to ePHI:

a. Employees shall not have access to workstations containing ePHI that are not in their respective Departments.
b. Visitors, contractors, staff, interns and volunteers will not have access to areas with workstations containing ePHI unless such access is required as part of the person's authorized activities at the Board's offices and the person is accompanied by a Board employee in such areas.
c. Employees shall be required to inquire about the status and access authorization of persons when that information is not known to the workforce member.
d. Measures such as changing of access codes, re-keying of locks, etc, shall be implemented when a workforce member having access to substantial amounts of ePHI is separated from employment.
e. Access to software for the purpose of testing and revision shall be limited to IT Department staff and authorized vendors/consultants.

3. **Maintenance Records:**

A record shall be created and maintained for modifications that occur to components of the Board's physical infrastructure that are essential to the security of ePHI, including but not limited to the changing of locks, changing of door combinations, installation/removal/repair of security devices, alteration/addition/removal of doors, routine maintenance checks.

a. A maintenance record must be created for each such modification made to the physical site, facility or building.
b. Such repairs and modifications shall be documented and maintained by the Security Officer.
c. All maintenance agreements for hardware and software, including installation, will be documented and maintained by the IT Department.
d. Maintenance agreements of all hardware and software will be reviewed on an annual basis.
e. Maintenance Records covered by this Section must be securely stored.

C. References: § 164.310(a).

II. <u>WORKSTATION USE AND SECURITY</u>: To establish guidelines for workforce members that will ensure the proper and use of workstations and prevent unauthorized use. These requirements shall be incorporated into the employee handbook.

A. General Guidelines

1. Workstations are the property of the Board and are only to be utilized for official Board business purposes during work hours. An exception is authorized for break periods (i.e. lunch). 2012 West 25th Street
2. All users have the responsibility to use workstations, information system resources and services in an efficient, effective, ethical and lawful manner and to be aware of the ways their own use might have adverse impact on other users.
3. All workforce members are expected to know and understand Board privacy and security policies and procedures, their obligations to protect the security, integrity and confidentiality with respect to all ePHI that resides on the Board's workstations and the associated networks and the sanctions that may be applied to workforce members for violations of such policies and obligations.
4. All workstations that access or contain ePHI shall be identified and inventoried (e.g. laptops, desktops, PDAs, etc).

5. Access of workstations that can access ePHI shall be limited to authorized users and shall be contained, whenever reasonably possible, in secure rooms where only authorized users work. All other workstations shall be situated in a manner to avoid being viewed by unauthorized users.
6. Files containing ePHI shall not be moved to removable media or a portable device unless the workforce member has received approval and complies with the parameters and purposes of the approval that has been granted.

B. Prohibited Uses

1. Unauthorized modification of computer resources, including the computer, computer software and information. *Modification* includes any unauthorized changes, appending, replacement, and contamination of the resources or any act that would make the resource inaccurate, unsuitable or unavailable for its intended use.

2. Any unauthorized attempt to obtain, provide or use a Board log-in ID or password that belongs to another user to log-onto or use any system.

3. Any use of Board-owned computer resources in the commission or attempted commission of a misdemeanor or felony crime or aiding, abetting, soliciting or conspiring to commit a computer-related crime.

4. Unauthorized use or access and/or attempted unauthorized use or access to Board information systems including but not limited to, all computers and information stored therein.

5. Unauthorized acquisition, disclosure, modification or destruction of any computerized information that supports Board business or the attempt to do so.

6. Attempting to disable, defeat or circumvent any Board supported-security feature or assisting anyone else in doing so.

C. User Privacy Expectations and Board Rights

1. System users are granted access to computer and information resources to assist them in performance of their jobs. Users do not have an absolute right to privacy in anything they create, send or receive on Board systems.
2. The Board desires to provide a reasonable degree of privacy to workforce members. At the same time, the Board retains the right to monitor usage of any and all aspects of its telecommunications and computer systems including user e-mail, voice-mail, networks, intranet and internet to ensure compliance with its policies and with relevant laws. This includes the right to perform manual or automated audits of system use and contents.
3. The email system is supported to facilitate business communications among and between participating authorized users and between workforce members and the Board's providers and business associates. While a user may have an individual mailbox and password on the system, the system in its entirety belongs to the Board, and the employee possesses no privacy interest or privacy expectation in the email account or system. The content of all email on the system is the property of the Board.
4. The Board reserves the right to review the contents of any user's email communications at any time, for any reason, without prior notification. Users should also be aware that workstation deletion of an email may not delete it from the email system and that deletion of emails may violate state record retention requirements related to public records.

D. User Security Obligations

1. Users are expected to be vigilant in maintaining system security and shall notify the Security Officer of any security weakness or breach.
2. Users must not break into or exceed authorized limits when accessing any computer network.
3. Users shall follow all account authorization and log-on/log-off procedures including logging-off before leaving workstation. Users shall not attempt to modify or disable automatic log-off settings.
4. Users shall maintain local passwords in accordance with the Board's procedures on passwords and follow password protection guidelines.
5. The Security Officer and/or Designees shall deploy virus and spyware protection software and all users shall follow current guidance on effective use procedures and optimal workstation settings for protection software.
6. Users shall take all reasonable precautions to avoid the entry or distribution of any malicious software (virus, Trojan Horse, worm, etc.) which may cause damage or any component of the Board's information systems.
7. No user shall connect any personal wireless network device to any computer system that accesses the Board's network, no matter where the computer is located (e.g., home, work, remote office, etc.).

E. **References** § 164.310(b) & (c).

III. DEVICE & MEDIA CONTROLS: To govern the receipt and removal of hardware and electronic media that hold ePHI into and out of the Board's offices and track their movement within the Board's offices. Such devices and media include hard drives, storage systems, removable disks, floppy drives, CD ROMs, PCMCIA cards, memory sticks, USB storage devices, and all other forms of removable media and storage devices.

A. Accountability

1. All electronic devices that have a data storage capability shall be identified and inventoried with notations as to location, assigned user(s), purpose of use and assignment dates. Inventories shall be retained for a minimum of six years.
2. The Security Officer or Designee shall record the receipt, removal and return of hardware and software containing ePHI.
3. No employee or user shall transfer ePHI to removable media or to any other portable device, with the exception of employees of the IT Department or employee who have been authorized in writing to do so by the Security Officer.
4. An exact retrievable copy of ePHI must be available on the Board's information systems prior to the movement of equipment, media or devices storing of that ePHI.
5. No employee or user shall remotely access ePHI except through the authorized us of a Board-issed ThinClient device.

B. Device and Media Re-Use

1. Prior to making storage devices and removable media available for reuse, IT Department staff shall ensure that the device or media does not contain ePHI.
2. If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to reuse.
3. If the device or media contains ePHI that is not required or needed, and is not a unique copy, an authorized data destruction protocol must be used to destroy the data on the device or media prior to reuse, if otherwise permitted by Board's record retention policies. Removable media that is used for system backup and disaster recovery and is stored and transported in a secured environment is not subject to the data destruction requirement.
4. IT Department staff will ensure that the previous label on such media that is to be overwritten is removed and destroyed.
5. Equipment that has residual value may be sold in accordance with Board financial policies once it has been properly cleaned of ePHI.
6. If the equipment has no residual value, cannot be reused, and ePHI has been stripped from it, then it should be recycled or disposed of in an environmentally safe manner.

C. Data Backup and Storage

1. Prior to disposing of or relocating any storage device or removable media, all ePHI shall be removed in accordance with approved data destruction protocols by IT Department staff.
2. If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to equipment disposal or equipment.
3. If the device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to equipment disposal or relocation.
4. Refer to the ***Data Backup Plan*** provision regarding the plan that the Board is required to have in place for the backup of its data.

D. Disposal

1. IT Department staff shall ensure that devices and media holding ePHI are properly disposed of when they are no longer needed by the current user and are ready to be transferred securely to a subsequent user, organization, or recycling company.
2. Prior to destroying or disposing of any storage device or removable media, IT staff shall ensure that the device or media does not contain ePHI.
3. If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI shall be made prior to disposal.
4. If the device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal.

E. Secure Data Removal Procedures

Media containing ePHI must have all of it irrevocably removed by IT Department or other Board staff using a method that ensures the ePHI cannot be recovered or reconstructed. Appropriate methods for destroying/disposing of data on various types of media are outlined in the following table.

Medium	Approved ePHI Destruction Method
Audiotapes	Methods for destroying/disposing of audiotapes include recycling (tape over) or pulverizing.
Hard Disk Drives	Methods of destruction/disposal should destroy data permanently and irreversibly. Methods may include overwriting data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten. Total data destruction does not occur until the back-up tapes have been overwritten.
Magnetic Media	Methods may include overwriting data with a series of characters or reformatting the tape (destroying everything on it). Total data destruction does not occur until the back-up tapes have been overwritten. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable.
Computer Diskettes	Methods for destroying/disposing of diskettes include reformatting, pulverizing, or magnetic degaussing.
CDR, RW, DVD	Disks used in "write once-read many" (WORM) document imaging cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
Microfilm/Microfiche	Methods for destroying/disposing of microfilm or microfiche include recycling and pulverizing.
PHI Labeled Devices	Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Removing labels or incineration of the medium would be appropriate.
Paper Records	Paper records should be destroyed/disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing.
Videotapes	Methods for destroying/disposing of videotapes include recycling (tape over) or pulverizing.

F. References: § 164.310(d).

/s/ Eugenia Kirkland

Eugenia Kirkland, LSW, MSSA, CDCA
ADAMHS Board Chair

3/28/18

Approval Date

/s/ Scott S. Osiecki

Scott S. Osiecki
Chief Executive Officer

03/2021

Review Date