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

POLICY STATEMENT

SUBJECT: SECURITY OF CLIENT INFORMATION – TECHNICAL SAFEGUARDS

EFFECTIVE DATE: MARCH 28, 2018

PURPOSE

The purpose of this policy is to describe the ADAMHS Board's Technical 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 Technical 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. ACCESS CONTROL To guard electronic protected health information (ePHI) from unauthorized access.

A. Unique User Identification

Each information system user shall be assigned a unique single name and/or number (User ID) for identifying and tracking user identity. Unique user identifiers will be used to track user activity within information systems that contain ePHI.

B. Emergency Access

Contingency procedures for authorized users to obtain necessary ePHI during an emergency shall be set forth in the Board's *Disaster Recovery and Emergency Mode Operations Plan*.

C. Automatic Logoff and Screen Saver

All workstations shall be set to automatically log-off users after fifteen minutes of inactivity. Users shall be instructed that it is a violation of the Board's Security Policy to deactivate or modify this setting.

D. Encryption/Decryption

The Board has considered the reasonableness and appropriateness of utilizing encryption and decryption for all ePHI *maintained* in its information systems to prevent access by unauthorized users or programs and has determined that it is not reasonable or appropriate for the Board to implement such safeguards as other safeguards and mechanisms will be adequate to protect such ePHI compared to the unreasonable burden that such safeguards would impose on the Board and its operations. (Note: This decision does not apply to encryption/decryption of *transmitted* ePHI addressed in Section V.)

E. References: § 164.312(a)(1).

II. AUDIT CONTROLS: To implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information (ePHI).

A. Audit Control Mechanisms

1. Every computer, communication device, program, or file that contains ePHI must utilize a mechanism to review the activity of programs and files that contain ePHI. Security Officer working with the IT Department staff must document the audit mechanisms that will be configured and implemented. Such mechanisms must allow for compliance with the Board's *Information System Activity Review Plan.*

2. Auditing shall be performed at a level determined to be appropriate by the Board's most current Risk Analysis.

3. Audit logs shall be captured at the application, system, and user level (i.e. Some individual applications may provide auditing while some may not, such as in the case of individual files or certain programs and databases, and will have to be audited at the operating system level.)

4. The audit log must include, at a minimum, the following information: User ID, Login Date/Time, and Service/Application/Information Accessed

5. Audit logs and audit trails will be safeguarded from unauthorized access.

6. Audit logs must be retained for a minimum of six years.

B. Audit Review Plan

Audit logs shall be reviewed/monitored in accordance with the *Information System Activity Review* procedures.

C. Audit Control Revisions

In the event that the ADAMHS Board's ePHI inventory or information systems should change, the audit mechanisms utilized must be revised accordingly to ensure compliance *(see Evaluation procedures under Administrative Safeguards).*

D. References: § 164.312(b).

III. INTEGRITY: To protect electronic protected health information (ePHI) from improper alteration or destruction.

A. Integrity Requirements

Security Officer working with the IT Department Staff will identify and document integrity requirements based on the results of its Risk Analysis and identification of scenarios that may result in modification to ePHI by unauthorized sources.

A. Integrity Assurance Methods

Security Officer working with the IT Department Staff must document the tools and techniques that have been identified and implemented to protect ePHI from unauthorized modification.

C. Data Authentication

Security Officer working with the IT Department Staff must document the authentication mechanisms that will be utilized to verify that ePHI has not been altered or destroyed in an unauthorized manner.

D. Integrity Monitoring
Data Integrity processes shall be evaluated periodically by Security Officer working with the IT Department Staff to determine whether integrity objectives are being met and whether revisions are necessary.

E. References: § 164.312(c).

IV. PERSON OR ENTITY AUTHENTICATION: To verify that a person or entity seeking access to electronic protected health information (ePHI) is the one claimed.

A. Authentication Mechanism
1. Users seeking access to any network, system, or application containing ePHI must verify their identity through the use of a unique user identification and password combination.

B. Prohibition against Misrepresentation
1. No person or entity seeking access to any Board network, system, or application shall misrepresent themselves by using another person or entity's identity such as the other person's User ID and Password.

2. No person or entity (other than a network or system administrator) shall allow unauthorized persons or entities to use their authentication credentials such as User IDs and passwords.

3. Employees engaging in misrepresentation of a person's identity shall be subject to the *Sanctions for Breach of Privacy and Security as identified in the Security of Client Information – Administrative Safeguards Policy.*

C. References: § 164.312(d).

V. TRANSMISSION SECURITY: To guard against unauthorized access and/or modification to electronic protected health information (ePHI) that is being transmitted over an electronic communications network.

A. Inner-Network Communications (Local Area Network [LAN] Traffic)
A VLAN will be utilized to minimize the possibility of traffic being intercepted and/or modified in transit on the LAN to help ensure that ePHI is only accessible to authorized users.

B. Employee Remote Access to LAN Resources
Remote Access is defined as any use of any Board internal LAN resource that originates from outside of the Board's LAN. An example would be an employee accessing files residing on a Board file server from their home computer. Authorized employees may only access Board internal LAN resources remotely in accordance with the *Remote Access* procedures. Remote access will occur through an encrypted virtual private network (VPN).

C. Agency Personnel Remote Access
Authorized contract provider personnel may only access the designated file drop off/report pick up file transfer server through a secure and authenticated method that complies with, as appropriate, NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated, and in accordance with the *Remote Access* procedures.

D. Transmission of ePHI Between Board and Outside Entities (such as other payers)
All ePHI transmissions between the Board and Outside Entities will be made through a securely encrypted and authenticated method that complies with, as appropriate, NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

E. Transmission of ePHI through E-mail or Messaging Systems
Any transmission of ePHI through E-mail or other insecure messaging systems (AOL IM, ICR, ICQ, Yahoo IM, etc.) is prohibited**.**

F. References § 164.312(e).

VI. REMOTE ACCESS: The purpose of this provision is to define standards for connecting to the Board's network from any host location. These standards are designed to minimize the potential exposure to the Board from damage that may result from the unauthorized use of the Board's resources including the loss of sensitive or company confidential data, damage to public image, and damage to critical internal systems

A. Applicability
1. These requirements apply to all Board employees, workforce members, contractors, providers, vendors, agents, and any other person or entity that has been authorized to remotely access the Board's LAN.

2. Remote access implementations and connections that are covered by this policy include, but are not limited to, reading or sending email, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

B. Remote Access Authorization
Remote access privileges shall only be granted, in accordance with the following, to persons who have received explicit authorization for such access by the Chief Executive Officer or the Security Officer:

1. Remote Access may be granted to contractors, vendors or agents on a temporary, as-needed basis, in order to facilitate the work of the Board.

2. Access and level of access granted will be specific to applications and business requirements.

3. Remote access control will be strictly controlled and monitored through password authentication. See the *Password Management* procedures identified in the *Security of Client Information – Administrative Safeguards Policy* for password requirements.

C. Remote Access User Requirements
1. Users shall ensure that their remote access connection is given the same security considerations as the user's on-site connection to ePHI.

2. Users are prohibited from providing their login or email password to anyone, including family members.

3. Users are prohibited from using non-Board email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Board business, thereby ensuring that official business is never confused with personal business. An exception is that Board IT department may use external email accounts to troubleshoot technical issues around email accounts.

4. Users shall not use personal devices or equipment for remote access purposes.

5. Users shall be given a copy of the requirements and obligations upon being granted remote access.

6. Users shall log-off when device and equipment are not in use.

D. Equipment and system requirements

IT Department staff shall ensure that Board-issued equipment and devices provided to users for remote access purposes comply with the following:

1. Operating systems are up-to-date with the latest security-related patches.

2. Anti-virus is software current and active.

3. Adequate password protection requirements, encryption and hardware and/or software firewall protections are utilized.

4. Automatic session termination after a period of inactivity is activated.

/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