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

**POLICY STATEMENT**

**SUBJECT: SECURITY OF CLIENT INFORMATION – ADMINISTRATIVE SAFEGUARDS**

**EFFECTIVE DATE: MARCH 28, 2018**

---

## PURPOSE

The purpose of this policy is to describe the Board's Administrative Safeguards for protecting the security of electronic personal health information (ePHI) that the 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 Administrative 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 Board's workforce.

**I. SECURITY MANAGEMENT PROCESS**: To implement procedures to prevent, detect, contain and correct security violations.

A. **Risk Analysis:** The Board shall conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of the Board's ePHI on a periodic basis.

1. The Security Officer shall ensure that a risk analysis is conducted on all information systems, processes and physical areas in Board offices and facilities to address changing threats, vulnerabilities, risks and organizational priorities. *(See References section of this policy for risk analysis resources that can be used to assist this effort)*
2. The Risk Analysis shall include the following steps:
    a Identify the Scope of the Analysis
    b. Gather Data and create inventory asset list (hardware, software, communication means) including each of the following:
        - Location of ePHI and how it is accessed, created, received, maintained or transmitted (internal and external)
        - Nature of the information and/or system
        - Business purpose
        - Operating environment
    c. Identify and document potential threats and vulnerabilities (human, natural, technology, other)
    d. Assess current security measures
    e. Determine likelihood of threat occurrence – high, medium, low
    f. Determine potential outcome of threat occurrence
    g. Determine Level of Risk
    h. Identify Security Measures
    i. Finalize Documentation

3. A Risk analysis shall be completed at least once every five years or when significant changes have occurred or are planned, before purchase or integration of new technologies, when changes are made to physical safeguards, when integrating technology and making physical security changes, and in response to environmental or operational changes affecting the security of ePHI.

4. External contractors or vendors may be utilized to conduct the analysis as necessary and appropriate.

5. References:

a. 164.308(a)(1)(ii)(A).

b. "Risk Management Guide for Information Technology Systems", Special Publication 800-30, NIST, Sept 2012 *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf*

**B. Risk Management:** The Board shall identify and implement security measures sufficient to reduce risks and vulnerabilities identified as part of its Risk Analysis to a reasonable and appropriate level.

1. The HIPAA Security Officer, in conjunction with the Risk Manager, shall ensure the development of a *Risk Management Plan* that identifies the security measures that are necessary to reduce risks and vulnerabilities identified by the Risk Analysis to a reasonable level appropriate to:
    a. Ensure the confidentiality, integrity and availability of ePHI;
    b. Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI;
    c. 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
    d. Ensure compliance with this policy and its procedures by the Board's workforce.

2. The plan shall implement a process for managing risks that:
    a. Defines "what" safeguards need to be established;
    b. Defines "how" they need to be established; and
    c. Measures compliance – periodic evaluation of the plan's implementation and its level of appropriateness to the current security environment.

3. If it is determined that a security measure recommended by the Risk Analysis will not be implemented to address a risk or vulnerability identified during a risk analysis, because the associated level of risk is at a reasonable and appropriate level, Chief Executive Officer and the Risk Manager or Security Officer must sign-off on the decision.

4. The Security Officer shall be responsible for ensuring implementation, maintenance and evaluation of identified security measures.

5. The Security Officer will maintain a copy of the Risk Analysis documents.

6. Risk management efforts and decisions as to what controls will and will not be put in place shall be documented and maintained for six years from their creation.

7. References:

a. 164.308(a)(1)(ii)

b. "Risk Management Guide for Information Technology Systems", Special Publication 800-30, NIST, Sept 2012 *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf*

**C. Information System Activity Review:** To ensure that information system activity is being monitored and reviewed appropriately.

1. The Security Officer and/or Designee shall oversee the inventorying of all systems that contain ePHI and that are used to access systems/servers that contain ePHI. The Security Officer and/or Designee shall maintain information system activity logs for such

2. An Information System Activity Review process shall be documented that includes the following:

    a. The audit controls, such as audit logs, audit trails and activity reports that will be used to track and manage system activity.

    b. The audit review process that will be utilized to review all audit logs and activity reports, including monitoring mechanisms, review frequency, review triggers and attention to known threats and vulnerabilities.

    c. Periodic testing to ensure logging mechanisms are working properly.

    d. Process for investigating and reporting security incidents and suspected rogue activity to the Security Officer.

    e. Notification by the Security Officer and/or Designee of appropriate personnel, management, security, and privacy personnel in the event of security incidents and/or suspected rogue activity.

3. References: § 164.308(a)(1)(ii)(D).

**D. Sanctions for Breach of Privacy and Security of PHI:** Appropriate sanctions shall be applied against workforce members who fail to comply with the ADAMHS Board's security policy and procedures as required by the Security Regulations and Ohio's Personal Information Systems Act.

1. All officers, employees, and agents of Board must adhere to these policies and standard and all supervisors are responsible for enforcing this policy. The Board will not tolerate violations of these policies and standards, and that such violations constitute grounds for disciplinary action up to and including termination, professional discipline, and criminal prosecution.

2. A statement of understanding of and adherence to this Security policy and procedures shall be signed by each new employee as a prerequisite to employment.

3. Any officer, employee, or agent of the Board who believes that another officer, employee, or agent of the Board has breached the Board's Security Policy, or the policies and standards promulgated to carry out the objectives of the Security Policy, or has otherwise breached the integrity or confidentiality of patient or other sensitive information, should immediately report such breach to his or her superior or to the Board's Security Officer.

4. Any allegation of violation of the HIPAA Security Rule or the Board's policies and procedures regarding the security of ePHI shall be made to the Board's Security Officer and/or Risk Manager. The Security Officer along with the Board's Risk Manager will conduct a thorough and confidential investigation into the allegations. The Board will inform the complainant of the results of the investigation and any corrective action taken. The Board will not retaliate against or permit reprisals against a complainant. Allegations not made in good faith, however, may result in discharge or other discipline.

a. When the investigation has been completed and a decision related to the allegations has been reached and implemented, the Officer shall notify the complainant of the results of the investigation and any corrective action taken.

b. "Whistleblower" Retaliation or Reprisals. The Board will not retaliate against or permit reprisals against an employee who reports either a violation to the integrity and confidentiality of a client's PHI or a potential breach or possible weakness to the security of the facilities or systems housing ePHI. Any workforce member involved in retaliatory behavior or reprisals against another workforce member for reporting such infractions shall be subject to disciplinary action.

c. Any employee who knowingly falsely accuses another of a violation of HIPAA rules and policy shall be subject to disciplinary action.

5. As stated in the Board's Human Resource Policy Manual, the Board has a progressive discipline policy under which sanctions become more severe for repeated infractions. This policy, however, does not mandate the use of a lesser sanction before the Board terminates an employee. In the discretion of management, the Board may terminate an employee for the first breach of the Board's Security Policy if the seriousness of the offense warrants such action.

6. Levels of HIPAA Violations
The following three (3) levels of violations will be utilized in recommending the disciplinary action and/or corrective action to apply:

***Level 1 Violations***
An employee inadvertently, mistakenly or accesses PHI that he/she has no need to know in order to carry out his/her job responsibilities or an employee carelessly uses or discloses information to which he/she has authorized access. Examples of level 1 HIPAA violations include, but are not limited to, the following:

- Leaving PHI in a public area;
- Mistakenly sending e-mails or faxes containing PHI to the wrong recipient;
- Discussing PHI in public areas where it can be overhead, such as the reception area, elevators, hallways, etc.;
- Leaving a computer accessible and unattended with unsecured PHI;
- Loss of an unencrypted electronic device containing unsecured PHI;
- An individual fails to report that his/her password has been potentially compromised (i.e., has responded to e-mail spam and given out their password);

***Level 2 Violations***
An employee intentionally accesses, uses and/or discloses PHI without appropriate authorization. Examples of level 2 HIPAA violations include, but are not limited to, the following:

- Intentional, unauthorized access to the employee's own PHI, or to that of friends, relatives, coworkers, or other individual's PHI (including searching for an address or phone number);
- Intentionally assisting another individual to gain unauthorized access to PHI. This includes, but is not limited to, the employee's giving another individual his or her unique user name and password to access electronic PHI;
- Disclosing consumer/patient condition, status or other PHI obtained by the employee to another workforce member who does not have a legitimate need to know;
- Failing to properly verify the identity of individuals requesting PHI which results in inappropriate disclosure, access or use of PHI;

- Engaging in intentional retaliatory behavior or reprisals against another workforce member for reporting HIPAA infractions.
- A second occurrence of any Level 1 violation (it does not have to be the same offense).

***Level 3 Violations***

- An employee intentionally uses, accesses and/or discloses PHI without any authorization and causes personal or financial gain; causes physical or emotional harm to another person; or causes reputational or financial harm to the Board. Examples of level 3 HIPAA violations include, but are not limited to, the following:
- Unauthorized intentional disclosure and/or delivery of PHI to anyone;
- Intentionally assisting another individual to gain unauthorized access to PHI to cause harm. This includes, but is not limited to, providing another individual with the employee's unique user name and password to access electronic PHI;
- Accessing or using PHI for the employee's personal gain (i.e., lawsuit, marital dispute, custody dispute);
- Disclosing PHI for financial or other personal gain;
- Using, accessing, or disclosing PHI when the disclosure results in personal, financial or reputational harm or embarrassment to a patient or provider;
- Second occurrence of any Level 2 violation (it does not have to be the same offense) or multiple occurrences of any Level 1 violation.

7. Disciplinary Actions

a. An employee could expect to lose his or her job for a willful or grossly negligent breach of confidentiality, willful or grossly negligent destruction of computer equipment or data, or knowing or grossly negligent violation of HIPAA, its implementing regulations, or any other federal or state law protecting the integrity and confidentiality of patient information, and may lose his or her job for a negligent breach of the Board's standards for protecting the integrity and confidentiality of patient information.

b. For less serious breaches, management may impose a lesser sanction, such as a verbal or written warning, verbal or written reprimand, loss of access, suspension without pay, demotion, or other sanction. In addition, the Board will seek to include such violations by contractors as a ground for termination of the contract and/or imposition of contract penalties.

c. The following shall serve as disciplinary guidelines:

- Level 1 violations shall result in counseling, an informal talk, oral warning and/or letter of reprimand.
- Level 2 violations shall result in a letter of reprimand, and may include imposition of disciplinary leave without pay and/or a recommendation for termination.
- Level 3 violations, in most cases, shall result in termination of employment.
- Violation of the Board's Security Policy may constitute a criminal offense under HIPAA, other federal laws, such as the Federal Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, or state laws. Any employee or contractor that violates such a criminal law may expect that the Board will provide relevant information concerning the violation to appropriate law enforcement personnel and will cooperate with any law enforcement investigation or prosecution.

- Violations of the Board's Security Policy or individual policies and standards may violate professional ethics rules and regulations applicable to an employee and may therefore be grounds for professional discipline. Any individual subject to professional ethics guidelines and/or professional discipline should expect the Board to report such violations to appropriate licensure or accreditation agencies and to cooperate with any professional investigation or disciplinary proceedings.

8. The Board will seek to include violations described in this section as grounds for termination of the contract and/or imposition of contract penalties.

9. In the event that the investigation reveals that the security of unsecured PHI was breached, the breach notification procedures set forth in the Board's *Policy on Privacy and Confidentiality of Client Information* shall be followed.

10. This Sanction Policy is intended as a guide for the efficient and professional performance of duties of the Board's officers, employees, and agents to protect the integrity and confidentiality of medical and other sensitive information. Nothing herein shall be construed to be a contract between the employer and the employee. Additionally, nothing in this Sanction Policy is to be construed by any employee as containing binding terms and conditions of employment. Nothing in this Sanction Policy should be construed as conferring any employment rights on employees or changing their legal status under Ohio law. Management retains the right to change the contents of this Sanction Policy as it deems necessary with or without notice.

11. References § 164.308(a)(1)(i)(C) and ORC §1347.05.

**II. <u>ASSIGNED SECURITY RESPONSIBILITY</u>**: To identify the ADAMHS Board's security officer and the security officer's responsibilities.

A. The role of the Board's Security Officer is assigned to the Chief Financial Officer.

B. The Security Officer is responsible for the development of the Board's Security policies and procedures, the oversight of their implementation and the specific additional responsibilities identified throughout these security procedures. Such duties and responsibilities shall be included in the Security Officer's main position description.

C. The name of the Security Officer, along with his or her assigned duties and responsibilities will be communicated to all members of the Board's workforce.

D. References: § 164.308(a)(2).

**III. <u>WORKFORCE SECURITY:</u>** To ensure that all authorized workforce members have appropriate access to ePHI, and to prevent workforce members who do not have authorization from obtaining access to ePHI.

**A. Workforce Authorization, Supervision and Clearance:** To ensure that the Board implements procedures to determine that the access of a workforce member to ePHI is appropriate.

1. The background of all Board workforce members must be adequately reviewed during the hiring process by the Director of Human Resources so that an administrative determination of trustworthiness can be made before allowing access to sensitive information.
    a. Proper background checks include, but are not limited to:
        (1) Confirmation of academic and professional qualifications
        (2) Professional license validation

(3) Criminal background check (BCI)
(4) Character references

b. The extent of the background check will be based on the workforce member's probable access to PHI or ePHI and their level of security responsibility.

c. When a workforce member is provided by an employment agency, the Board's Director of Human Resources will determine whether the agency's screening process is adequate or whether additional background checks are necessary.

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

3. New employees shall be trained with respect to security policies and procedures prior to having access to PHI.

4. A workforce member that is promoted or transferred and have substantially greater responsibility for or access to PHI and ePHI shall be trained with respect to privacy and security policies and procedures, as is appropriate to their duties.

5. A workforce members' access to PHI or ePHI shall be determined based upon job responsibilities, amount and type of supervision required and other factors as determined by the appropriate Executive Staff member. Board workforce members shall only be authorized to have access to PHI and ePHI, and the locations where it resides, as is necessary for the individual to competently perform the duties and responsibilities of their position, as determined necessary by the Board's assessment of position-related duties and needs.

6. Security responsibilities and the extent of a workforce members' access to PHI and ePHI will be documented though the use of group permissions established by active directory and/or the database or server housing the ePHI. "Security responsibilities" include general responsibilities for implementing or maintaining security of PHI and ePHI, as well as any specific responsibilities for protecting and maintaining the confidentiality, integrity, and availability of information systems or processes such as when Remote Access privileges have been grated

7. References: §§ 164.308(a)(3)(ii)(A) and (B).

**B. Workforce Termination:** To provide for the termination of access to ePHI and PHI when the employment of a workforce member ends or his/her position changes and when terminating a business associate relationship.

1. The appropriate Executive Staff Member must notify the Security Officer when access is no longer appropriate as a result of the occurrence of any of the above. The Security Officer shall:

a. Deactivate or eliminate user accounts immediately upon separation unless authorized personnel provide other instructions.

b. Ensure that departing workforce member cannot damage any computerized systems and that any locked files they may have can be opened by authorized personnel.

c. Block access privileges (both physically and electronically) immediately, if necessary.

d. Provide access to workforce member's user account to relevant supervisor.

e. Ensure the changing of combination locks and/or collection of key cards, keys or any other facility access control mechanisms, if necessary.

f. Address the disposition of the affected workforce member's electronic media, within a reasonable amount of time. If necessary, backups of all systems that the affected workforce member has had access to will be made for administrative control.

g. If changing work duties requires an alteration of access to PHI or ePHI:
   i. Access related to previous work duties must be terminated.
   ii. Establishment of new PHI and/or ePHI access is to be based on established access and clearance policies.

2. The Director of Human Resources will collect all agency assets (e.g. computers, cell phones, pages, etc.) and distribute those assets to the appropriate staff for accounting, review, and redistribution.

3. References: § 164.308(a)(3)(ii)(C).

**IV. INFORMATION ACCESS MANAGEMENT:** To authorize access to ePHI that are consistent with the requirements of the HIPAA Privacy Regulations and the ADAMHS Board's *Policy on Privacy and Confidentiality of Client Information.*

**A. Access Authorization, Establishment and Modification:** To govern the granting of access to workstations, transactions, programs, processes, or other mechanisms containing ePHI and to establish, document, review and modify a user's right of access to such ePHI. Authorized user may include a workforce member, contract provider, subcontractor, vendor, and/or auditor.

**B. Granting Access:** Access shall be authorized according to the work and/or business-related needs of each person/entity as determined by position description and specific assignments/activities.

1. System Access requests shall be initiated by a member of the Board's Executive Team submitting a completed ***Security Access Form*** to the Security Officer for review.

2. The Security Officer shall consider requests for access in accordance with the Workforce Authorization, Supervision and Clearance requirements.

**C. Modifying Access**

1. Modification of access privileges can be accomplished through the use of a ***Security Access Form*** in accordance with the Access Authorization and Modification requirements. Access changes must be submitted in writing to the Security Officer, with a specific date and time that access modification is effective. , the system will be updated to reflect the user's authorized access level.

2. The appropriate Executive Staff Member shall submit a ***Security Access Form*** to the Security Officer to modify access upon the following personnel events:

- New Hire
- Reassignment or promotion
- Resignation
- Suspension
- Termination

- Disciplinary action involving curtailment of access to computer resources
- Conclusion of a temporary employment engagement
- Conclusion of a consultative engagement
- Conclusion of a volunteer assignment involving access to computer resources

3. A member of the Board's Executive Team shall submit a ***Security Access Form*** to the Security Officer to modify access based upon a workforce member's change in position and/or work-related duties or a outside entities/persons change in Board-related activities and/or authorization.

4. Requests for termination of user access shall be affected immediately upon notification by the Director of Human Resources.

5. It is the responsibility of the requestor to notify the workforce member of access modifications.

6. References § 164.308(a)(4)(ii)(B) and (C).

**V. <u>SECURITY AWARENESS AND TRAINING:</u>** To establish and implement a security awareness and training program for the ADAMHS Board's workforce.

**A. Security Training Program:**

1. The Director of Risk Management, in collaboration with the Security Officer, shall develop training materials to be utilized for the Board's staff training program.

2. Training provided shall be based on workforce member's responsibilities level of access and interaction with ePHI and shall address issues regarding the use, access and security of ePHI.

3. Staff training shall be provided as follows:
    a. General security awareness or targeted training to new workforce members within 90 days of their employment, depending on roles and responsibilities.
    b. General security awareness training to all workforce members on an annual basis
    c. Specific security training to affected workforce members within 60 days of environmental or operational changes that affect the security of ePHI (e.g. new or revised policies and procedures, new or upgraded software, new security technology, changes to information systems, revisions to the Security Rule, etc.)

4. The Security Officer shall retain records of each training provided, sign-in sheets and copies of training materials.

5. References: § 164.308(a)(5)(i).

**B. Security Reminders:** Security Reminders shall be utilized to help staff effectively participate in the Board's security program by periodically reminding them of best practices and individual responsibilities.

1. The Security Officer and IT Department staff are responsible for staying apprised (through trade magazines, subscription services, continuing education, etc) of new system vulnerabilities as they become known.

2. The Security Officer shall ensure the distribution of periodic notices and reminders to the workforce regarding:
    a. The Board's Security policy and procedures and legal requirements to keep information secure and confidential.
    b. Changes to Board Security policies and procedures.
    c. Threats, breaches, or vulnerabilities that have been discovered or reported that may compromise or affect ePHI and/or PHI.
    d. Best security practices for specific staff or departments.
3. General reminders about workforce member's obligations for security will be posted visibly in common as well as areas where ePHI is stored, processed or transmitted.
4. Notices and reminders will be made available via email, postings in common areas and areas where ePHI is stored, processed or transmitted and via staff meetings, as appropriate.
5. Provision of security reminders and notices shall be documented to include the type of reminder, summary of message and date.
6. References: § 164.308(a)(5)(ii)(A).

**C. Guarding Against, Detecting and Reporting Malicious Software:** To detect and report on the intrusion of malicious software such as viruses, Trojan horses or worms. Malicious software can be the source of system security breaches and can also compromise the integrity and validity of the data stored in such systems.

1. Security Officer working with the IT Department Staff must implement safeguards to protect Board systems from malicious software. Such safeguards will include at a minimum, the following:

a. A virus detection system must be implemented on all workstations including a procedure to ensure that the virus detection software is maintained and up-to-date. Antivirus technology that updates automatically, without user intervention, should be implemented, as well as systems for logging, notifying IS administrators in the event of virus outbreaks.

b. Operating system practices that prevent users from downloading or installing software applications.

c. Firewall and or SPAM control policies that prevent non-approved files from being procured by or pushed out to users.

d. Anti-spyware software to assist in mitigating the affects of such rogue software.

e. Ensuring that the latest Board approved and purchased operating systems, as well as application software patches, are installed on all workstations and servers.

2. The Security Officer and the IT Department staff must stay current in knowledge of new vulnerabilities and threats from malicious software.

3. The Security Officer must ensure that the workforce is trained and educated at least annually to become participants in the identification of and protection against malicious software.

4. Each user must notify the Security Officer, in writing, if they believe rogue software has been installed on their workstation. Such written correspondence must describe what software has been installed, how the software was installed (by email or by visiting a specific website) and when the software was installed. A search will then be performed to determine if the software was installed elsewhere.

5. Each user must notify the Security Officer, in writing, if the employee becomes aware of a virus, worm, or other malicious code that has comprised or potentially compromised ePHI. Such written correspondence shall describe under what conditions the virus was activated. Thereafter, the employee must immediately follow the instruction of IT Department personnel in responding to the threat, including instructions to relinquish control of his or her workstation to IT Department personnel.

6. The HIPAA Security Officer is responsible for maintaining a form on which such notifications are recorded. The form shall be forwarded to the Chief Executive Officer and the HIPAA Privacy Officer.

7. In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation, that system must be disconnected from the network until the system has been appropriately cleaned.

8. References: § 164.308(a)(5)(ii)(B).

**D. Log-in Monitoring:** To ensure that access to servers, workstations, and other computer systems containing ePHI is appropriately maintained and that patterns of intrusion attempts can be monitored and analyzed.

1. Log-in attempts shall be logged and reviewed to identify and report suspicious log-in activity.

2. All log-in attempts to systems containing ePHI will be captured with the following information being collected:

a. Log-in
b. System
c. Computer name (and or IP address)
d. Success or Failure
e. Date/Time

3. All failed attempts deemed as suspicious must be logged and reported to the Security Officer and/or Designees for further investigation as outlined in the *Security Incident Response and Reporting* procedures.

4. Systems shall be set to require resetting of a password after 3 incorrect log-in attempts.

5. References:

a. § 164.308(a)(5)(ii)(C)
b. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

**E. Password Management:** To ensure unique and reliable identification of individual information system users and to minimize the likelihood of improper access or use by establishing a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

1. All users of the Board's information systems are required to present their system user name along with a self-constructed password or passwords in order to access workstations.
2. Workforce training and reminders shall include how to safeguard passwords.
3. Users shall keep their individual passwords safe from discovery and must not divulge them to anyone.

4. Users must only employ passwords that meet the following specifications:
   a. Length: eight (8) or more characters
   b. Contents: Passwords and pass phrases combine at least three of the four following keyboard character types:
      - upper case alphabetic characters (A, B, C . . . .)
      - lower case alphabetic characters (a, b, c . . . .)
      - numerals (0 – 9)
      - special characters (e.g., @, #, &, ~)
   c. Passwords must not be a variation of the user's actual name or the username, the name of the Board, etc.
   d. Passwords must not be based on any easily guessed characteristic of the user.
5. Passwords must be changed at least every 90 days and when a user suspects that his/her password has been compromised.
6. When changing passwords, previous passwords may be re-used no more often than every twelfth time and the new password must be substantially different from the previous one.
7. If a user records a password, the password must be recorded in a location that is unlikely to be discovered by an unauthorized person.
8. Users who forget a system password should contact the IT Department for assistance.

9. Users must immediately report discovered or stolen passwords to the Security Officer. The Security Officer shall provide instruction to the user about how to better secure future passwords.

10. IT Department Staff shall periodically scan for old or inactive user accounts and take appropriate actions including but not limited to reviewing directory and removing terminated employees, and scheduling recurring appointment to review on calendar every month.

11. References: § 164.308(a)(5)(ii)(D).

**VI. SECURITY INCIDENT RESPONSE AND REPORTING:** To appropriately address security incidents that threaten the privacy, integrity, or availability of information stored on its information systems.

1. Security Incidents include, but are not limited to:
Attempted or actual violations of Board information system security policies, particularly those that compromise or threaten to compromise electronic protected health information or other non-public information maintained by the Board.
- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- Unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Infection by virus or other malicious software
- Failure of system hardware, firmware, or software
- Breaches of ePHI

2. Workforce members and other persons/entities having a contractual relationship with the Board shall be required to report any potential security events of which they are aware to the Security Officer or Risk Manager. methods for monitoring activity on its information systems.

3. The Security Officer and/or Designee are responsible for reviewing and reporting on all threats, breaches, and concerns that have been discovered or reported that may affect ePHI or PHI.

4. The Security Officer shall be responsible for assessing reports of unusual security events, evaluating their degree of threat, and initiating and coordinating the appropriate level of response.

5. The Risk Manager, Security Officer and IT Department shall jointly develop and document Security Incident Processes for reporting and addressing incidents at each level (i.e. user to Executive Director), and for prioritizing and documenting incidents.

6. An annual calendar year report of security incidents shall be produced by the Security Officer and distributed to Executive Council.

7. All Security Incident reports shall be retained for 6 years.

8. References § 164.308(a)(6).

**VII. CONTINGENCY PLAN:** To respond to an emergency or other occurrence that damages systems that contain ePHI.

**A. Data Back-up Plan**: To establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

1. IT Department staff shall document and implement a ***Data Backup Plan*** that specifies which data, drives or resources on each server or workstation are backed-up, how often, by whom, and the type of back-up to be performed.

2. All users shall be required to store all mission critical workstation data on the servers in the users' assigned folders. This will insure that the user data is backed up and available if the user's workstation crashes.

3. At least the most current full backup shall be stored off-site in a secure manner. The off-site location must be far enough away that it would not be affected by the same building disaster (i.e. fire or tornado).

4. A backup log shall be kept showing what data/server/workstation was backed-up, when the data was backed-up, what method was used, and on what backup media the data is located.

5. Logs will be kept that record what was backed-up, when, the method used and on what backup media the data is located.

6. Periodically, data will be restored from back-up media to test that the backup hardware, software, media, and process is working correctly and that data can be recovered as intended. Data from each backup media shall be validated as part of the backup process

7. References: § 164.308(a)(7)(ii)(A).

**B. Disaster Recovery Plan and Emergency Mode Operation Plan:** To assist in the restoration of any loss of data and to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

1. Security Officer working with IT Department staff must document and implement a ***Disaster Recovery Plan and Emergency Mode Operations Plan*** that specifies, at a minimum, the following:

- Disaster and emergency classifications
- Prioritization of responses
- Disaster recovery tasks and assigned responsibility for each
- Contingency procedures for continuing vital operations
- Preventative measures
- Facility access plans
- Data restoration tasks and responsibility
- Location of Plans at alternate locations
- Phone number and contact names for all persons that must be notified in the event of a disaster

2. Workforce members must be familiar with the contents of this plan and follow its guidance, as appropriate, in a disaster or emergency situation.

3. References**:** § 164.308(a)(7)(ii)(B) and (C).

**C. Testing and Revision Procedures:** The Board's ***Disaster Recovery Plan and Emergency Mode Operations Plan s***hall be periodically evaluated for its continued applicability and effectiveness in response to environmental and operational changes.

1. IT Department Staff shall evaluate its Plans annually or when environmental and operational changes occur, by conducting, at a minimum, each of the following:

    a. Testing procedures

    b. Reviewing the existing list of equipment that stores ePHI, and update it to reflect current status annually**.**

    c. Restoring data from storage media to test that the backup hardware, software, media, and process is working correctly.

    d. Reviewing its list of vendors, employees, and contacts at the state and verify that these are still appropriate.

    e. Using scenario-based walk-throughs and/or performing complete live tests.

2. References: § 164.308(a)(7)(ii)(D)

D. **Application and Data Criticality Analysis:** Security measures must be appropriate to the criticality and sensitivity of Boards ePHI, its applications, and its operations.

1. Security measures must be matched to the criticality and sensitivity of the assets they protect. Security level designations are used to set the requirements for the security efforts the Board takes to protect its information assets. They are based on an analysis of the:

a. Sensitivity of data maintained on them, and
b. Operational criticality of individual data systems.

2. IT Department Staff shall evaluate its information systems to determine the security measures appropriate to each and to ensure the continuity of critical data processing capabilities.

3. IT Department Staff shall develop a Security level Framework that identifies security level designations based on:

a. The sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse).

b. The operational criticality of data processing capabilities (i.e., the ramifications if data processing capabilities were interrupted for a period of time or subject to fraud or abuse).

c. Ensuring that security plans are reasonable and appropriate in light of the assigned security level designations.

4. References § 164.308 (a)(7)(i)(E).

**VIII. EVALUATION: To periodically evaluate the extent to which the Board's security policy and procedures meet the requirements of the Security Regulations.**

**A.** The Board shall conduct technical and non-technical evaluations of its security plans and procedures to ensure that its ePHI is being adequately protected.

**B. Timing of Evaluations:**

1. IT Department Staff will review the Board's security policies and procedures and their continued applicability in response to environmental and operational changes affecting the security of ePHI (i) when new technology is implemented to verify that no vulnerabilities to ePHI are created from the adoption of the new technology. in response to the identification of new risks, (ii) vulnerabilities or changes to the Board's infrastructure, data or systems and in any event and (iii) at least every 24 months.

2. Documentation of technical and non-technical evaluations shall be made and retained.

**C.** Where reasonable and appropriate, the Board will contract with an external entity to perform this evaluation.

**D.** Documentation of technical and non-technical evaluations shall be made and retained.

**E. References:**

a. § 164.308(a)(8).
b. NIST self-evaluation tool: scap.nist.gov/hipaa

**IX. BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS: To set forth the security-related requirements that must be included in a Business Associate Agreement or Memorandum of Understanding that is entered into by the Board.**

**A. Required Assurances:** When a Business Associate Agreement (BAA) or Memorandum of Understanding (MOU) is entered into pursuant to the Board's Business Associate requirements *(See Policy on Privacy and Confidentiality of Client Information)*, the BAA or MOU must contain the following satisfactory assurances by the Business Associate related to the security of ePHI:

1. Business Associates (BA) will appropriately safeguard the ePHI.

2. BAs will report to the Board any security incident of which it becomes aware, including breaches of unsecured ePHI as required by HIPAA's Breach Notification Rules (45 CFR 164.410)

3. BAs will comply with the applicable requirements of HIPAA's Security Regulations.

4. BAs will require any subcontractors that maintain, create, receive or transmit ePHI on behalf of the BA to comply with the applicable requirements of HIPAA's Security Regulations.

**B. References:** §§ 164.308(b), 164.314(a) and 164.504(e)(2).

**X. <u>POLICY AND PROCEDURES</u>** To ensure policies and procedures are implemented, reviewed and updated as required by the Security Regulations.

**A. Security Officer Requirements:**

1. Make the Board's security policies and procedures available to the respective members of the Board's workforce that are responsible for their implementation.

2. Audit the implementation of the Board's Security policies and procedures on a periodic basis to ensure compliance.

3. Review the Board's Security policies and procedures on an annual basis, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.

4. Document changes to the Board's Security policies and procedures and oversee implementation of such changes.

B. **References:** § 164.316.

**XI. <u>DOCUMENTATION REQUIREMENTS</u>** To ensure that documentation is maintained and retained as required by the Security Regulations.

A. The Board's Security Policy and procedures shall be maintained in written (which may be electronic) form.

B. A written record shall be maintained of any actions, activities or assessments required to be documented by the Board's Security Policy and procedures.

C. The Board's Security policies and procedures and all written actions, activities and assessments shall be retained for a minimum of 6 years from date of creation or date when last in effect, whichever is later.

D. **References:** § 164.316.

**<u>REFERENCES</u>**

*ADAMHS Board Policy on Privacy and Confidentiality of Client Information*

Security Regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR Parts 160, 162, and 164 Subpart C

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

HHS Security Rule Guidance Material and Educational Paper Series

https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

"Information Security: An Introductory Resource Guide for Implementing the HIPAA Security Rule", Special Publication 800-66, National Institute for Standards and Technology (NIST), Oct 2008
*http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf*

"Risk Management Guide for Information Technology Systems", Special Publication 800-30, NIST, Sept 2012
*http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf*

"Recommended Security Controls for Federal Information Systems", Special Publication 800-53, NIST
*http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

"Guide for Mapping Types of Information and Information Systems to Security Categories, (Vol. 2)", Special Publication 800-60, NIST *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf*

*/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**