

**ADAMH BOARD OF FRANKLIN COUNTY  
HIPAA Privacy Policy H.01.020**

**BUSINESS ASSOCIATES**

**A. PURPOSE STATEMENT**

The purpose of this policy is to issue instructions to all ADAMH workforce members regarding the necessity for and the required content of agreements with business associates relating to the business associate's receipt of protected health information from or on behalf of ADAMH workforce members.

**B. SCOPE**

This policy applies to all ADAMH workforce members, including Board of Trustees members, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for ADAMH, is under the direct control of ADAMH, regardless of whether they are paid by ADAMH.

**C. POLICY STATEMENT**

1. Generally:

a. Contract Providers:

- i. ADAMH contract providers furnishing treatment services are covered entities, and no business associate agreement is required.
- ii. ADAMH contract providers not furnishing treatment services (such as prevention, peer support, employment readiness, housing, or advocacy entities) are not covered entities under the HIPAA regulations. To the extent protected health information is disclosed to these contract providers by ADAMH, they are business associates and a business associate agreement is required.

b. ADAMH may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if ADAMH obtains satisfactory assurance that the business associate will appropriately safeguard the protected health information.<sup>1</sup> This requirement does not apply with respect to: disclosures made to a provider concerning the individual's treatment, or uses or disclosures made to another governmental agency for purposes of public benefit eligibility or enrollment determinations where such agency is authorized by law to make these determinations.

c. ADAMH must document these assurances through a written agreement or as follows<sup>2</sup>:

- i. If the business associate is another governmental entity, the entity may comply with this requirement by executing a memorandum of understanding or like document covering the required terms or by relying on other law that imposes upon the business associate the requirements specified herein.
- ii. If the business associate is required by law to perform a function, activity, or service on behalf of ADAMH, ADAMH may disclose protected health information to the extent necessary to comply with that mandate as long as the entity documents an attempt to obtain the required assurances and the reasons that such assurances could not be obtained.

---

<sup>1</sup> CFR Title 45, Section 164.502(e)(1) Standard: Disclosures to business associates

<sup>2</sup> CFR Title 45, Section 164.502(e)(2) Standard: Implementation specification: Documentation

**ADAMH BOARD OF FRANKLIN COUNTY  
HIPAA Privacy Policy H.01.020**

- d. The business associate, by virtue of signing the business associate agreement, acknowledges that they have the same level of responsibility regarding protection and security of protected health information as any HIPAA covered entity. If a violation occurs, the business associate is subject to the same mitigation requirements.
2. Content Requirements of a Business Associate Agreement
- a. The agreement between ADAMH and the business associate must meet the following requirements, as applicable<sup>3</sup>:
    - i. Establish permitted and required uses or disclosures of protected health information that are consistent with those authorized for ADAMH, except that the agreement may permit the business associate to use or disclose protected health information for its own management and administration, if such use or disclosure is required by law or the business associate obtains reasonable assurance that the confidentiality of the protected health information will be maintained.
      - (a) A business associate shall, in all cases, limit use or disclosure of protected health information to the limited data set, if practicable, or, if needed by the business associate, the minimum amount of protected health information necessary to perform the task or accomplish the purpose of the use or disclosure;
      - (b) A business associate may not de-identify protected health information created, received or maintained by business associate under the agreement, except as necessary to provide service under the agreement or as requested by ADAMH. Protected health information created, received or maintained by a business associate which has been de-identified at the request of ADAMH may not be used by the business associate for any purpose not expressly approved by ADAMH;
      - (c) A business associate may not aggregate protected health information created, received or maintained by the business associate under the agreement, whether de-identified or not, with any other protected health information, including without limitation protected health information of the business associate's other customers.<sup>4</sup>
    - ii. Provide that the business associate will:
      - (a) Not use or further disclose the protected health information except as authorized under the agreement or required by law;
      - (b) Use appropriate administrative, staff education, technical, electronic, and physical safeguards to prevent unauthorized use or disclosure;
      - (c) Report unauthorized uses or disclosures to ADAMH, including any breach of unsecured protected health information, cooperate with ADAMH in investigating any breach, take reasonable steps to mitigate the potentially harmful effects of any breach, document those steps, and indemnify ADAMH for any losses and damages which are the result of business associate's or an

---

<sup>3</sup> CFR Title 45, Section 164.504(e) – Standard: Business associate contracts

<sup>4</sup> See items II A, II B, and II D (Restrictions on Use and Disclosures of Protected Health Information) in the ADAMH business associate agreement template.

**ADAMH BOARD OF FRANKLIN COUNTY**  
**HIPAA Privacy Policy H.01.020**

agent or subcontractor of business associate's breach of protected health information;

- (d) Pass on the same obligations relating to protection of protected health information to any subcontractors or agents, and set forth these obligations in their own business associate agreement with the subcontractor. The business associate must send a copy of this agreement to ADAMH;
- (e) Make protected health information available for access by the individual or his or her personal representative, in accordance with relevant law and policy;
- (f) Make protected health information available for amendment, and incorporate any approved amendments to protected health information, in accordance with relevant law and policy;
- (g) Make information available for the provision of an accounting of uses and disclosures in accordance with relevant law and policy;
- (h) Make its internal practices, books and records relating to its receipt or creation of protected health information available to the Office of the U.S. Secretary of Health and Human Services for purposes of determining the entity's compliance with HIPAA regulations;
- (i) If feasible, return or destroy all protected health information upon termination of contract; if any protected health information is retained, continue to extend the full protections specified herein as long as the protected health information is maintained;
- (j) Within one day of discovery, report to ADAMH any security incident relating to electronic protected health information of which business associate becomes aware;
- (k) Adopt written policies and procedures consistent with business associate's obligations;
- (l) Not use or disclose protected health information in any manner that would not be permissible if used or disclosed by ADAMH.

- iii. Authorize termination of the agreement by ADAMH upon a material breach by the business associate (This element of the agreement may be omitted if the business associate is another governmental entity and the termination would be inconsistent with the statutory obligations of ADAMH or the business associate.)

3. Security Requirements<sup>5</sup>

- a. A business associate has the same responsibility to secure protected health information that any HIPAA covered entity has, which include such general responsibilities for implementing or maintaining security of ePHI, as well as any specific responsibilities for protecting and maintaining the confidentiality, integrity, and availability of information systems or processes as ADAMH has, including, but not limited to, the following:
  - i. Protected health information in paper form must be physically secured by locked file cabinets and rooms.

---

<sup>5</sup> §164.306 – Security standards: General rules

**ADAMH BOARD OF FRANKLIN COUNTY**  
**HIPAA Privacy Policy H.01.020**

- ii. Business associate staff must use only the minimum necessary information needed to perform their task. Workforce members' access to protected health information should be restricted dependent on job duties and the type of supervision required.
          - iii. Protected health information in electronic form (ePHI) must be secured with encryption or other secure electronic means regarding communication and storage.
            - (a) PHI must not be electronically transmitted in a non-secure manner (over an open internet without encryption). Protected health information must never be sent using typical e-mail.
            - (b) E-mail with protected health information should not be accepted unless sent in an electronically secure manner.
        - b. A business associate must adhere to the security regulations established under HIPAA. This includes establishing and maintaining security measures such as the following:
          - i. Internal management and audits of information system activity including system login/logoff; password security; database access; firewall; e-mail; Web server; Enterprise anti-virus; spy ware; spam activity logs;
          - ii. Adequate workforce training regarding needed paper and ePHI confidentiality;
          - iii. Secure data backup measures;
          - iv. Protective and recovery procedures regarding protected health information protection during a disaster.
4. Breach Requirements<sup>6</sup>
  - a. Any impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate demonstrates a low probability that the protected health information has been compromised or an exception applies.
  - b. A business associate shall handle a breach of confidentiality by notifying the ADAMH Board immediately upon discovery and pay the costs associated with notifying individual(s) whose information protection has been breached within 60 days of discovery and the media when appropriate. ADAMH reserves the right to control the process for notifying individuals affected by the breach.
5. Oversight Responsibilities
  - a. If ADAMH knows of a material breach of the agreement or violation of HIPAA, ADAMH must require the business associate to cure the breach or end the violation and, if such attempt is unsuccessful, terminate the agreement, if feasible, and, if not, report the problem to the Office of U.S. Secretary of Health and Human Services.

---

<sup>6</sup> §164.410 – Notification by a business associate