


**COUNTY OF IMPERIAL  
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES  
POLICY AND PROCEDURE MANUAL**

<b>SUBJECT:</b> HIPAA - Business Associates	<b>POLICY NO:</b> 01 88
<b>SECTION:</b> Administration	<b>EFFECTIVE DATE:</b> 9-17-21
<b>REFERENCE:</b> 45 C.F.R. Subtitle A, Subchapter C, Parts 160 and 164	<b>PAGE:</b> 1 of 18
<b>AUTHORITY:</b> Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	<b>SUPERSEDES:</b> 6-8-16  <b>APPROVED BY:</b>  

**PURPOSE:** To establish a policy regarding the identification of and contracting with outside entities that perform services for or on behalf of ICBHS for which they receive protected health information (PHI) and are considered to be "business associates" under HIPAA.

**SCOPE:** The information in this document applies to all members of the workforce which includes employees, contract employees, volunteers, trainees, etc., granted access to protected health information (PHI).

**NOTES:** On January 17, 2013, the U.S. Department of Human Services (HHS) released the omnibus regulations under the Health Insurance Portability and Accountability Act (HIPAA), including implementing changes made by the Health Information Technology for Economic and Clinical Health Act (HITECH). Some of the changes affect business associates and subcontractors of business associate.

The original HIPAA rules applied only to covered entities (health care providers utilizing electronic transactions, health plans, and health care clearinghouses). HIPAA had an indirect application to business associates, because the HIPAA rules required a covered entity to enter into a written agreement with the covered entity's business associate which required the business associate to protect the security and privacy of PHI. One of the most significant changes introduced by the HITECH Act was to apply the security provisions of HIPAA directly to business associates.

Business associates are now directly liable for violation of the HIPAA Security Rule, and for uses and disclosures of PHI in violation with the Privacy Rule. Business associates also have the following responsibilities:

1. To keep records and submit compliance reports to HHS, when HHS requires such disclosure in order to investigate the business associate's compliance with HIPAA, and to cooperate with complaint investigations and compliance reviews;
2. To disclose PHI as needed by a covered entity to respond to an individual's request for an electronic copy of his/her PHI;
3. To notify the covered entity of a breach of unsecured PHI;
4. To make reasonable efforts to limit use and disclosure of PHI, and requests for PHI, to the minimum necessary;
5. To provide an accounting of disclosures; and
6. To enter into agreements with its subcontractors which comply with the HIPAA Privacy and Security Rule.

Previously, the HIPAA rules required that the business associate contract provide that the business associate ensure that any agent, including a subcontractor, receiving PHI would agree to the same restrictions that apply to the

business associate. Now, agreements between business associates and their subcontractors will have to meet all elements required for a business associate agreement with the covered entity.

Business associate agreements have provided that the business associate must report to the covered entity uses or disclosures of PHI not provided for in the business associate's contract; now, the business associate must report inappropriate uses and disclosures, including breaches of unsecured PHI. Business associates must also agree to comply with Subpart C of the HIPAA rules (dealing with compliance and investigations). Also, to the extent that the business associate is responsible for carrying out any of the covered entity's responsibilities under the HIPAA rules (such as responding to patient requests for copies of their records), the business associate is required to comply with the provisions of the HIPAA rules that would apply to the covered entity in carrying out that function.

A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

**DEFINITIONS:**

**Administrative Safeguards:** Administrative actions and policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the County's or business associate's workforce in relation to the protection of that information.

**Breach:** The acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule. A breach does not include:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity if made in good faith and within the scope of the authority, with no further use or disclosure;
2. Any inadvertent disclosure by a person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, to any authorized person, and the PHI is not further used or disclosed;
3. Any disclosure of PHI where the covered entity or business associate has a good faith belief the unauthorized person would not reasonably have been able to retain such information.

The covered entity or business associate must be able to demonstrate that there is a low probability that the information has been compromised based on a risk assessment of at least the following:

1. The nature and extent of the PHI involved, including the identifiers;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

**Business Associate:** A person or entity, who on behalf of the covered entity, and other than in the capacity of a workforce member who performs or assists in the performance of an activity that involves the use or disclosure of PHI who provides certain functions, activities or services for or to ICBHS involving the use or disclosure of PHI. Examples includes entities that provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

Disclosures of PHI by ICBHS to a health care provider for treatment purposes are not considered a business associates function.

**Business Associates Agreement:** A legally binding agreement entered into by a covered entity and business associate that established permitted and required uses and disclosures of protected health information, provides obligation for the business associate to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is material breach.

**Data Aggregation:** means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

**Designated Record Set:** A group of records maintained by or for a covered entity that:

1. Are the medical records and billing records about Individuals maintained for or by a covered health care provider;
2. Are the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for health plan; or
3. Are used in whole or in part by or for the covered entity to make decisions about individuals.

For purposes of this definition, the term record means any item, collection or grouping of information that includes PHI and is maintained, used, collected or disseminated by or for a covered entity.

**Disclosure:** The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

**Electronic Protected Health Information:** Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

**Health Information Organization (HIO):** Performs activities on behalf of one or more HIPAA covered entities to manage the exchange of PHI through an electronic network. In that role, HIOs are defined by HIPAA as Business Associates of the covered health care providers. Also known as a Health Information Exchanges (HIEs), they may be governmental, non-profit or for profit organizations.

**Physical Safeguards:** Physical measures, policies, measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

**Protected Health Information (PHI):** Individually identifiable information relating to past, present, or future physical or mental health condition of an individual, provision of health care to an individual, or the past, present, or future payment for health care provided to an individual transmitted or maintained in any form or medium including oral, written, or electronic communication.

**Required by Law:** Means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care

providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

**Security Incident:** Means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operation in an information system. "Security incident" does not include trivial incidents that occur on a daily basis, such as scans, "pings", or unsuccessful attempts to penetrate computers networks or services maintained by the business associate.

**Technical Safeguards:** Means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

**Unsecured PHI:** Unsecured PHI means PHI that is not rendered unusable, unreadable, undecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services.

**Use:** With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within ICBHS.

**Workforce:** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the department, is under the direct control of the department, whether or not they are paid by the department.

**POLICY:** Imperial County Behavioral Health Services (ICBHS) will identify business associate relationships and, prior to disclosing an individual's PHI to such business associates, enter into a written business associate agreement in accordance with the provisions set forth below. Copies of all business associates agreements are to

be submitted to the ICBHS Privacy Officer/designee. The ICBHS Privacy Officer/designee is responsible for maintaining all business associates agreements ICBHS enters into.

A. **Business Associates**

With respect to ICBHS, a person or organization who, on behalf of ICBHS or of an organized health care arrangement in which the ICBHS participates, but other than in the capacity as a member of the ICBHS workforce, creates, receives, maintains or transmits protected health information for a function or activity, including the following:

1. A function or activity involving the use or disclosure of protected health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing benefit consulting management, practice management, and repricing; or
2. Provides, other than in the capacity of an ICBHS workforce member, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for ICBHS, or for an organized health care arrangement in which ICBHS participates, where the provision of the service involves the disclosure of protected health information from ICBHS, or from another business associate of ICBHS, to the person.

The HIPAA Omnibus Rule (Final Rule) changed the definition of business associate to include:

1. A Health Information Organization, E-prescribing Gateway, or other person or organization that provides data transmission services with respect to protected health information to the and that requires routine access to such protected health information; and



2. A person or entity who offers a personal health record to one or more individuals on behalf of the ICBHS.
3. A subcontractor who performs a function for a business associate requiring access or use of PHI.
4. A person who creates, receives, or *maintains* or transmits PHI on behalf of a covered entity.

A covered entity participating in an organized health care arrangement that performs a function or activity as described in A.1. of this definition or that provides a service as described in A.2. of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

**B. Exceptions to a Business Associates Relationship**

A business associate relationship does not exist, even though an outside entity may receive PHI from ICBHS in order to perform a function or activity for or on ICBHS' behalf, in the following instances:

1. Treatment. A business associate relationship does not exist when ICBHS discloses PHI to another health care provider for purposes of treatment.
2. Financial Transactions. A business associate relationship does not exist between ICBHS and a financial institution if the financial institution only processes consumer-related financial transactions for the purpose of health care payment.
3. Disclosures between a group health plan and plan sponsor. A business associate relationship does not exist between a group health plan and plan sponsor.
4. Organized health care arrangements. Entities that participate in an organized health care arrangement

are not business associates of each other.

5. Entities Acting as Mere Conduits. A business associate relationship does not exist between ICBHS and entities acting as mere conduits in the transmission of PHI such as the US Postal Service or a courier service).
6. Service provider for non-medical equipment. (e.g. plumbers, electricians, photocopy services)

**C. Identification of Business Associates Relationships**

Prior to entering into any new relationship with outside entities, ICBHS will evaluate whether such relationships will constitute business associate relationships by:

1. Identifying whether the outside agency will perform a function or activity for or on behalf of ICBHS
2. Determining whether the entity will receive PHI from ICBHS in the performance of such function or activity

**Note:** A business associate relationship is formed only if protected health information is used, created, maintained or transmitted in the relationship.

Examples of business associates include:

1. Consultants and independent contractors with access to PHI
2. Software and hardware provider who accesses PHI for installation, maintenance and support services
3. Records management company (storage)

**D. Contracting Requirements of Business Associate Agreements**

Where ICBHS has identified that a business relationship exists, and an exception does not apply, then ICBHS will enter into a written business associate agreement.

Such agreements will contain the following provisions:

1. Obligations and Activities of Business Associate:

Business associate agrees to:

- a. Not use or further disclose PHI except as authorized or as required by law; § 164.504(e)(2)(ii)(A)
- b. Use appropriate safeguards with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided by its contract; § 164.504(e)(2)(ii)(B)
- c. To comply with the HIPAA Security Rule at Subpart C of 45 CFR Part 164 with respect to electronic PHI ICBHS discloses to business associate or business associate creates receives maintains, or transmits on behalf of ICBHS;
- d. To mitigate, to the extent practicable, any Harmful effect that is known to business associate of a use or disclosure of PHI by business associate that is in violation of the requirements of this agreement; § 164.504
- e. Report to ICBHS any unauthorized use or disclosure of the information provided for by its contract of which it becomes aware including breaches of unsecured protected health information; § 164.504(e)(2)(ii)(C)
- f. Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information; § 164.504(e)(2)(ii)(D) and § 164.314(2)(i)(B)

**Note:** ICBHS is not required to obtain satisfactory assurances from a business associate that is a subcontractor of ICBHS' business associate.

- g. Provide access to PHI, at the request of ICBHS, and in time and manner designated by ICBHS, to ICBHS or as directed by ICBHS, to the individual in accordance with §164.524; § 164.504(e) (2) (ii) (E)
- h. Make PHI in the designated record set available for amendment and incorporate any amendments in accordance with §164.526. Business associate will notify ICBHS no later than ten (10) calendar days after amendment is completed; § 164.504(e) (2) (ii) (F)
- i. Make its internal records relating to the use and disclosure of protected health information received from or created by or received by the business associate on behalf of ICBHS, available to the Secretary of Health and Human Services (DHHS) for the purposes of determining ICBHS' compliance; §164.504 (e) (2) (ii) (H)
- j. Make available the information required to provide an accounting of disclosures in accordance with § 164.528, Accounting of disclosures of protected health information; § 164.504(e) (2) (ii) (G)
- k. Provide ICBHS or an individual, as directed by ICBHS, in a time and manner directed by ICBHS, that information collected in accordance with this agreement, in order to permit ICBHS respond to request by an individual for an accounting of disclosure in accordance with § 164.528;
- l. Work with ICBHS upon notification by business associate to ICBHS of a breach to proper determine if any breach exclusions exists.

## 2. Security Rule

An agreement between ICBHS and a business associate must also provide that a business associate agrees to:

- a. Implement and maintain appropriate administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives maintains, and transmits on behalf of ICBHS.
- b. Ensure that any subcontractors that creates, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree through a contract with the business associate to the same restrictions and requirements required of the business associate. § 164.314(2)(i)(B)

**Note:** ICBHS does not have a statutory obligation to monitor the activities of its business associates. ICBHS, however, must respond to reported privacy breaches and security incident events should they occur and take reasonable steps to cure any potential breach or end the violation.

- c. Business associate shall report to ICBHS immediately any security incident of which it becomes aware. § 164.314(2)(i)(C) Business associate shall report breaches of unsecured PHI in accordance as required by § 164.410.

**Note:** If a covered entity (ICBHS) and the business associate are both government entities, additional implementation specification must be address (See 45 C.F.R § 164.504 (e)(3)).

## 3. Permitted Uses and Disclosures

The business associate may use or disclose PHI ICBHS perform functions, activities, or services

for, or on behalf of, ICBHS as specified in the agreement, provided that the use or disclosure would not violate the HIPAA Privacy Rule if done by ICBHS except that:

- a. The business associate may use PHI ICBHS discloses to business associate, if necessary for proper management and administration of business associate.
- b. The business associate may disclose PHI ICBHS discloses to business associate for the proper management and administration of business associate or to carry out the legal responsibilities of business associate, if:
  - 1) The disclosure is required by law; or
  - 2) Business associate obtains reasonable Assurance from the person to whom PHI was disclosed that it will be held confidentially and used or further disclosed only as required by law or for purposes for which it was disclosed to the person and the person immediately notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.
  - 3) Business associate may use and further disclose PHI ICBHS discloses to business associate to provide data aggregation services relating to the health care operations of the business associate.
- c. Business associate may use PHI ICBHS discloses to business associate, if necessary, to carry out legal responsibilities.
- d. Business associates may use and disclose PHI ICBHS discloses to business associate

consistent with the minimum necessary policies and procedures of ICBHS.

- e. Business associates may use or disclose PHI ICBHS discloses to business associates as required by law.

#### 4. Breach Discovery and Notification

Following the discovery of a breach of unsecured PHI, a business associate shall notify ICBHS immediately; however, the notification will be delayed if advised by law enforcement official pursuant to § 164.412.

- a. A breach is considered discovered by a business associate as of the first day on which such breach is known to the business associate, or by exercising reasonable diligence, would have been known to the business associate.
- b. The business associate is deemed to have knowledge of a breach if the breach is known or by exercising reasonable diligence would have been known, to any person who is an employee, officer, or other agent of the business associate.
- c. The business associate shall provide the notification of a breach to the ICBHS Privacy Officer. The notice shall include, to the extent possible:
  - 1) The identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been accessed, acquired, used, or disclosed during the breach; and
  - 2) Any other information that ICBHS is required to include in the notification to the individual under § 164.404(c), including:

- a) A brief description of what happened, Including the date of the breach and the date of the discovery of the breach, if known;
  - b) A description of the types of unsecured PHI that were involved in the breach (such as full name, social security number, date of birth, home address account number, diagnosis, disability code, other types of information were involved);
  - c) Any steps the individual should take to protect themselves from potential harm resulting from the breach;
  - d) A brief description of what the business associate is doing to investigate the breach, to mitigate harm to the individuals, and to protect against any future breach;
  - e) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address Web site, or postal address.
- 3) ICBHS may require the business associate to provide notices to the individual as required in § 164.404, if it is reasonable to do so under the circumstances.
  - 4) In the event that the business associate is responsible for a breach of unsecured PHI in violation of the HIPAA Privacy Rule, the business associate has the burden of demonstrating that the business associate made all notifications to ICBHS consistent with this paragraph D above and as required by breach notification regulations, or in the alternative that the



acquisition, access, use, or disclosure of PHI did not constitute a breach.

- 5) A business associate shall bear all expenses or other costs associated with the breach and shall reimburse ICBHS for all expenses ICBHS incurs in addressing the breach, including costs of investigation, notification, remediation, documentation of other costs associated with addressing the breach.

**Note:** Any subcontractor of the business associate that provide services to the business associate has the same responsibilities regarding reporting unauthorized uses or disclosures as the business associate.

5. Obligations of ICBHS in Business Associate Relationships

- a. Notify business associate of any limitation(s) in ICBHS' Notice of Privacy Practices in accordance with §164.520, to the extent that such limitation may affect the business associates use and disclosure of HI.
- b. ICBHS will notify the business associate of any changes in, revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect the business associates use and disclosure of PHI.
- c. ICBHS will notify business associate of any restrictions to the use or disclosure that ICBHS has agreed to in accordance with 164.522, to the extent that the restriction may affect the business associates use or disclosure of PHI.
- d. ICBHS shall not request that business associate to use or disclose PHI in a manner that would not be permissible under the HIPAA Privacy Rule if done by ICBHS.

6. Business Associate Termination

- a. Upon ICBHS' knowledge of a material breach or violation by a business associate of, ICBHS shall:
  - 1) Provide the business associate an opportunity to cure the material breach or end the violation within 30 days; or
  - 2) Immediately terminate the agreement.  
*§ 164.504 (e) (2) (iii) and § 164.314 (2) (i) (D)*
- b. Upon termination of the contract, the business associate shall either return or destroy all protected health information received from, or created, maintained, or received by the business associate on behalf of ICBHS. The business associate shall retain no copies of such information.
- c. If such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. *§ 164.504(e) (2) (ii) (H)*.
- d. The obligations of the business associate agreement shall survive the termination of the agreement.