



**COUNTY OF SAN BERNARDINO  
STANDARD PRACTICE**

**No. 14-03 SP 08**

**PAGE 1 OF 4**

**EFFECTIVE DATE** June 10, 2016

**POLICY: HIPAA POLICY  
SP: Business Associate Agreements**

**APPROVED**  
GREGORY C. DEVEREAUX  
Chief Executive Officer

**PURPOSE**

To establish guidelines regarding agreements between the County and Business Associates in accordance with the Health Insurance Portability and Accountability Act (HIPAA).

**DEPARTMENTS AFFECTED**

All County agencies, departments and Board-governed Special Districts that are determined to be covered by HIPAA.

**DEFINITIONS**

*Business Associate:* A person or organization that on behalf of a covered entity, other than a member of the covered entity's workforce creates, receives, maintains, or transmits Protected Health Information (PHI).

*Covered Entity:* A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA covered transaction.

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

*Electronic Protected Health Information (ePHI):* Protected health information in electronic form.

*Health Care Component (HCC):* County departments or programs that meet the definition of a Covered Entity or Internal Business Associate.

*Health Insurance Portability and Accountability Act (HIPAA):* A federal law designed to provide privacy and information security standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. (45 C.F.R. Parts 160 and 164)

*Internal Business Associate:* A County department or program that provides services to another County department or program covered by HIPAA that if it was a separate legal entity would fall within the definition of a Business Associate.

*Privacy Rule:* Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. (45 C.F.R. Part 164 Subpart E).

*Protected Health Information (PHI):* Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium (excludes individually identifiable health information in employment records held by Covered Entity in its role as employer).

*Security Rule:* Establishes national standards to protect individuals' ePHI that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. (45 C.F.R. Part 160, and Part 164 Subparts A and C.)

**PROCEDURES**

- A. Except as provided in paragraph D., business associate means, with respect to a covered entity, a person who:
1. On behalf of such covered entity, or an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by 45 C.F.R. Parts 160, 162 or 164, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. section 3.20, billing, benefit management, practice management and repricing; or
  2. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the services involves the disclosure of PHI from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
- B. A covered entity may be a business associate of another covered entity.
- C. Business associate includes:
1. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a covered entity and that requires access on a routine basis to such PHI.
  2. A person that offers a personal health record to one or more individuals on behalf of a covered entity.
  3. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.
- D. Business associate does not include:
1. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
  2. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or Health Maintenance Organization with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 C.F.R. section 164.504(f) apply and are met.
  3. A government agency with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.
  4. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph A.1. of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph A.2. of this definition to or for such organized health care arrangement by virtue of such activities or services.
- E. **Health Care Component (HCC) departments shall consult with County Counsel to resolve questions with respect to business associate relationships.**

- F. An HCC department may allow a business associate to create, receive, maintain, or transmit PHI on the HCC department's behalf only if the HCC department obtains satisfactory assurances, that the business associate will appropriately safeguard the information in compliance with the provisions below. An HCC department is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

**Written Contract or Other Arrangement:** HCC departments must document the satisfactory assurances through a written contract or other arrangement with the business associate that meets the following requirements:

1. *Business Associate Contracts:* The contract must:

- a. Establish the permitted and required uses and disclosures of PHI by the business associate.
- b. Provide that the business associate will:
  - i. Not use or further disclose the information other than as permitted or required by contract or law;
  - ii. Use appropriate safeguards and comply, where applicable, with the HIPAA Security Rule with respect to ePHI, to prevent use or disclosure of the information other than as provided for by the contract;
  - iii. Report to the HCC department any use or disclosure of the information not provided for by the contract of which it becomes aware, including breaches of unsecured PHI;
  - iv. 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;
  - v. Make available PHI in accordance with 45 C.F.R. section 164.524;
  - vi. Make available PHI for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. section 164.526;
  - vii. Make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. section 164.528;
  - viii. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the department available to the Secretary of Health and Human Services for purposes of determining the HCC department's compliance with HIPAA; and
  - ix. At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the HCC department that the business associate still maintains in any form and retain no copies of such information or, 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.

- c. Authorize termination of the contract by the HCC department, if the HCC department determines that the business associate has violated a material term of the contract.
2. *Other Arrangements*: If the business associate is a governmental entity, the HCC department may comply with this requirement by entering into a memorandum of understanding with the business associate that contains the terms that meet the objectives listed above. Arrangements between an HCC department and an internal business associate must be documented in a memorandum of understanding that complies with this Standard Practice.
3. *Performance Required by Law*: If a business associate is required by law to perform a function or activity on behalf of the HCC department or to provide a service described in the definition of a business associate by 45 C.F.R. section 160.103 to an HCC department, the HCC department may disclose PHI to the business associate to the extent necessary to comply with the legal mandate without a contract, provided the HCC department attempts in good faith to obtain satisfactory assurances in accordance with section F.1. above.
4. *Limited Data Sets*: The HCC department may comply with these requirements if the HCC department discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the HCC department has a data use agreement with the business associate that complies with 45 C.F.R. sections 164.514(e)(4) and 164.314(a)(1), as applicable.
5. *Countywide Template*: A countywide business associate agreement template has been developed as a guideline for HCC departments and may be accessed on the Human Resources Office of Compliance and Ethics website.

This Standard Practice shall not be construed as relieving departments of their responsibility to develop full and complete departmental policies, procedures, and practices necessary to expand and tailor this overall County Policy to the particular needs of their departments.

**LEAD DEPARTMENT**

Human Resources