

Business Associate Agreement checklist

INSTRUCTIONS: The following is the text:

1. 160.103 (containing the definition of Business Associate),
2. 164.502 (containing the Business Associate requirement)
3. 164.504 (containing the required elements of a Business Associate agreement), and
4. December 4/2002 Guidance (which explains the transition requirements).

Check off each element if reviewing a Business Associate agreement, to make sure it contains the required elements.

160.103

Business associate:

1. Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:
 1. On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
 1. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
 2. Any other function or activity regulated by this subchapter; or
 2. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), 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 service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
2. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) 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.
3. A covered entity may be a business associate of another covered entity.

164.502 (e)

1. **Standard: disclosures to business associates.**
 - i. A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory

Business Associate Agreement checklist

assurance that the business associate will appropriately safeguard the information.

- ii. This standard does not apply:
 - A. With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;
 - B. With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or
 - C. With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.
 - iii. A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.504(e).
2. Implementation specification: documentation. A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

164.504 (e)

1. **Standard: business associate contracts.**

- i. The contract or other arrangement between the covered entity and the business associate required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2) or (e)(3) of this section, as applicable.
- ii. A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (e) of this section, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
 - A. Terminated the contract or arrangement, if feasible; or
 - B. If termination is not feasible, reported the problem to the Secretary.

CHECKLIST OF REQUIRED ELEMENTS

2. Implementation specifications: business associate contracts. A contract between the covered entity and a business associate must:
- i. Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:
 - A. The contract may permit the business associate to use and disclose protected health information for the proper management and

Business Associate Agreement checklist

- administration of the business associate, as provided in paragraph (e)(4) of this section; and
- B. The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
- ii. Provide that the business associate will:
 - A. Not use or further disclose the information other than as permitted or required by the contract or as required by law;
 - B. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
 - C. Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
 - D. Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;
 - E. Make available protected health information in accordance with § [164.524](#);
 - F. Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § [164.526](#);
 - G. Make available the information required to provide an accounting of disclosures in accordance with § [164.528](#);
 - H. Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and
 - I. At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity 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.
 - iii. Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.
3. Implementation specifications: other arrangements.
- i. If a covered entity and its business associate are both governmental entities:
 - A. The covered entity may comply with paragraph (e) of this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section.
 - B. The covered entity may comply with paragraph (e) of this section, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section.
 - ii. If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § [160.103](#) of this subchapter to a covered entity, such covered entity may disclose protected health information to the business

Business Associate Agreement checklist

- associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph (e), provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(3)(i) of this section, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.
- iii. The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.
4. Implementation specifications: other requirements for contracts and other arrangements.
- i. The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:
 - A. For the proper management and administration of the business associate; or
 - B. To carry out the legal responsibilities of the business associate.
 - ii. The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:
 - A. The disclosure is required by law; or
 - B.
 - 1. The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and
 - 2. The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

December 12/04/2002 Guidance

Transition Provisions for Existing Contracts. Covered entities (other than small health plans) that have an existing contract (or other written agreement) with a business associate prior to October 15, 2002, are permitted to continue to operate under that contract for up to one additional year beyond the April 14, 2003 compliance date, provided that the contract is not renewed or modified prior to April 14, 2003. This transition period applies only to written contracts or other written arrangements. Oral contracts or other arrangements are not eligible for the transition period. Covered entities with contracts that qualify are permitted to continue to operate under those contracts with their business associates until April 14, 2004, or until the contract is renewed or modified, whichever is sooner, regardless of whether the contract meets the Rule's applicable contract requirements at 45 CFR 164.502(e) and 164.504(e). A covered entity must otherwise comply with the Privacy Rule, such as making only permissible disclosures to the business associate and permitting individuals to exercise their rights under the Rule.