

## BUSINESS ASSOCIATE AGREEMENT (Satisfactory Assurances) A Checklist for Providers

### The regulations established the following requirements for the Business Associate Agreement (Satisfactory Assurances):

Business Associate Agreement must:

- \_\_\_\_\_ Be in writing.
- \_\_\_\_\_ State permitted and required uses and disclosures.
- \_\_\_\_\_ Prohibit uses and disclosures not allowed in the Business Associate Agreement or by law or that would be a violation of the Privacy Regulations if done by the Covered Entity (CE).
- \_\_\_\_\_ Require Business Associate (BA) to use appropriate safeguards to prevent any unauthorized use or disclosure.
- \_\_\_\_\_ Require BA to report to the CE any unauthorized use or disclosure of which BA becomes aware.
- \_\_\_\_\_ Require that, any agents, including a subcontractor, to whom BA provides protected health information received from the CE, or created or received by BA on behalf of the CE, agree to the same restrictions and conditions that apply to the BA with respect to such protected health information unless disclosures are required by law or unless disclosures are for BA's proper management or administration and BA obtains the "reasonable assurances" described below from such downstream user.
- \_\_\_\_\_ Require BA to make available protected health information to the Individual in the Designated Record Set in accordance with 45 C.F.R. §164.524. [\[While these provisions must be in the Business Associate Agreement, actual access is not required if Business Associate does not possess protected health information in the original Designated Record Set. See, Sample Business Associate Contract Provisions, paragraph \(f\), 67 F.R. at p. 53265.\]](#)
- \_\_\_\_\_ Require BA to make available and to incorporate any amendment to protected health information in the Designated Record Set in accordance with 45 C.F.R. §164.526. [\[While these provisions must be in the Business Associate Agreement, actual amendment is not required if Business Associate does not possess protected health information in the original Designated Record Set. See, Sample Business Contact Provisions, paragraph \(g\), 67 F.R. at p. 53265.\]](#)
- \_\_\_\_\_ When requested by CE, require BA to make available to CE the information required to allow the CE to provide an accounting of disclosures in accordance with 45 C.F.R. §164.528.

\_\_\_\_\_ Require BA to make its internal practices, books, and records available to the Secretary of Health and Human Services for purposes of determining the CE's compliance with the Privacy Rule to the extent related to the uses and disclosure of protected health information received from, or created or received by the BA on behalf of, the CE .

\_\_\_\_\_ Require return or destruction of protected health information at end of contract, if feasible; but, if return or destruction is not feasible, extend the protection of the BA Agreement to the information and limit further uses and disclosures to the purposes listed in the BA Agreement.

\_\_\_\_\_ Authorize termination of Agreement if BA violates material term of Business Associate Agreement.

### **Optional Terms**

\_\_\_\_\_ This Business Associate Agreement may permit the BA to use PHI for the proper management and administration of the BA or to carry out its legal responsibilities.

\_\_\_\_\_ The Business Associate Agreement may permit the BA to disclose protected health information if needed for the proper management and administration of the BA or to carry out the legal responsibilities of the BA if:

1. The disclosure is required by law,

or,

2. The BA obtains reasonable assurances from the person to whom PHI is disclosed that the PHI will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person and the person agrees to notify the BA of any instances of which it is aware in which the confidentiality of the PHI has been breached.

\_\_\_\_\_ The Business Associate Agreement may allow BA to provide Data Aggregation Services relating to CE's health care operations.

\_\_\_\_\_ The Business Associate Agreement may define Protected Health Information.

\_\_\_\_\_ The Business Associate Agreement may define Designated Record Set.

**Reminders:**

1. If CE has entered into an agreement prior to October 15, 2002, and if the agreement does not expire or is not renegotiated between October 15, 2002 and April 14, 2003, then such Agreement does not have to include the HIPAA Business Associate Agreement (Satisfactory Assurances) until the earlier of:
  - a. the date the Agreement is renewed or renegotiated; or,
  - b. April 14, 2004.
2. "Evergreen Contracts," those that renew automatically without any change in terms or other action by the parties, and that exist prior to October 15, 2002, are eligible for the "extension" explained in #1 of this section. The automatic renewal does not terminate qualification for the additional time for compliance.
3. The Appendix to the final modifications to the HIPAA Privacy Rule issued August 14, 2002 (67 F.R. 53,182 *et seq.*) contain sample Business Associate Agreement provisions. *See*, 67 F.R. 53,262-53,266. Be aware, they are not sufficient in and of themselves to create a binding contract.

***THIS DOCUMENT SHOULD BE CONSIDERED ONE EXAMPLE OF HOW AN ORGANIZATION CAN START THEIR COMPLIANCE EFFORTS- IT IS INTENED TO BE USED SOLELY AS A VEHICLE FOR DISCUSSION TO HELP COMAPANIES DEVELOP THEIRM OWN COMPLIANCE MATERIAL. THIS DOCUMENT IS PROVIDED AS GENERAL GUIDANCE AND DOES NOT CONSTITUTE LEGAL ADVICE. COMPANIES SHOULD CONTACT THEIR OWN LEGAL COUNSEL TO TAILOR THE DOCUMENT TO MEET THEIR SPECIFIC NEEDS.***