Business Associate Agreement Checklist – Required and Optional Terms

Required Terms The following terms **must** appear in a Business Associate Agreement ("BAA").		
Regulatory Requirements	**Notes**	**Check-off**
164.502(e)(1)(i): **Basic Principle**: A Covered Entity ("CE") may disclose Protected Health Information ("PHI") to a business associate ("BA") and may allow a business associate to create, receive, maintain or transmit PHI on its behalf so long as a BAA is in place.		
164.504(e)(2):	**Notes**	**Check-off**
(i) **Identify – By Listing or Referring to Services Agreement:** Establish the permitted and required uses and disclosures of PHI by the BA.		
BA Can't do what CE Can't do: The contract may not authorize the BA to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the CE, except for the optional management/administration and data aggregation provisions listed in the "Optional Terms" section of this checklist.		
(ii) Provide that the BA will:	**Notes**	**Check-off**
(A) **Use/Disclose:** Not use or further disclose the information other than as permitted or required by the contract or as required by law.		
(B) **Safeguards:** Use appropriate safeguards and comply, where applicable, with the HIPAA Security Rule (Subpart C of 45 C.F.R. Part 164) with respect to Electronic PHI, to prevent use/disclosure of information other than as provided for by the BAA.		
(C) **Reports/Breach:** Report to the CE any use or disclosure of the information not provided for by its contract, or any Security Incident, of which it becomes aware, or any Breaches of Unsecured PHI as required by 45 C.F.R. § 164.410.		
(D) **Subcontractors**: Ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the BA agree in writing to the same restrictions and conditions that apply to the BA with respect to such information.		
(E) **Access**: Make available PHI in accordance with § 164.524;		
(F) **Amendments**: Make available PHI for amendment and incorporate any amendments to PHI in accordance with §164.526;		
(G) **Accounting**: Make available the information required to provide an accounting of disclosures in accordance with § 164.528;		
Accounting: Track information needed for an accounting.		
(H) **Privacy Rule.** To the extent BA is to carry out any of CE's obligations under the Privacy Rule, comply with the requirements of the HIPAA Privacy Rule (Subpart E of 45 C.F.R. Part 164) that apply to CE in the performance of such obligations.		
(I) **Records**: Make its internal practices, books, and records relating to		

Required Terms The following terms **must** appear in a Business Associate Agreement ("BAA").		
Regulatory Requirements	**Notes**	**Check-off**
the use and disclosure of PHI received from, or created or received by the BA on behalf of, the CE available to the Secretary for purposes of determining the CE's compliance with the Privacy Rule;		
(J) **Return/Destroy**: At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by BA on behalf of, the CE that the BA 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.		
Termination Provision: Authorize termination of the contract by the CE, if the CE determines that the BA has violated a material term of the contract.		

Optional Terms The following terms often appear, but are not required to be in, a BAA. Their inclusion is often a matter of negotiating power and/or leverage between the CE and BA.		
Term	**Notes**	**Check-off**
Mgmt/Admin of BA: The contract may permit the BA to use and disclose PHI for the proper management and administration of the BA: **USE** if necessary: (A) For the proper management and administration of the BA; or (B) To carry out the legal responsibilities of the BA. **DISCLOSE** if (A) The disclosure is required by law; or (B)(1) The BA 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 BA of any instances of which it is aware in which the confidentiality of the information has been breached.		
Data Aggregation: The contract may permit the BA to provide data aggregation services relating to the health care operations of the CE.		
"Suspected Breaches": Requirement that BA inform CE of a "suspected" Breach of Unsecured PHI and permit CE to engage in breach analysis.		
Broader Uses/Disclosures: Any permitted uses or disclosures of PHI that are broader than those listed in the Checklist above as "Required Terms." This may include, for example, permitting the use or disclosure of PHI for marketing, fundraising, de-identification, limited data sets or research purposes. The BA is not permitted to engage in these activities unless the CE has given BA permission to do so.		
More Specific Restrictions: Provisions specifically addressing BA's		

Optional Terms The following terms often appear, but are not required to be in, a BAA. Their inclusion is often a matter of negotiating power and/or leverage between the CE and BA.		
Term	**Notes**	**Check-off**
obligations under HIPAA with respect to marketing, fundraising, adhering to restrictions on disclosures, selling PHI, minimum necessary policies and procedures and other restrictions that apply to BA regardless of whether they are mentioned in the BAA.		
Indemnification: Indemnification provisions (one-way or mutual).		
Insurance: Insurance by BA to protect CE against BA's violations.		
Third Party Beneficiaries: Third party beneficiaries created or prohibited.		
Assignment: Assignment prohibited or permitted.		
Audits: Provisions obligating BA to allow CE to engage in periodic audits or inspections of the BA		
Penalties; Injunctions: Imposition of penalties in the event of a breach or unauthorized disclosure of PHI by BA, such as liquidated damages, or provisions establishing specific performance/equitable relief for CE in event of a violation.		
Representations: Warranties and representations that BA complies with HIPAA Security Rule and applicable provisions of Privacy Rule.		
HITECH Amendments: Commitment by BA to comply with HITECH-based regulatory changes to HIPAA provisions in the future.		
Workforce: Agreement by BA that its workforce will comply with applicable HIPAA provisions.		
Mitigation: Requirement that BA mitigate any harmful effects of impermissible use/disclosure.		
Restrictions on Subcontractors: As an alternative to the "Subcontractors" provision in the "Required Terms" section above, CEs may prohibit BAs from using subcontractors altogether or may attempt to require BA to use a particular form of Subcontractor BAA with subcontractors. CEs may prohibit BA from using subcontractors that are outside of the U.S. or not subject to jurisdiction in U.S. courts.		
Notifications: Provisions under which CE informs BA about: (1) CE's notice of privacy practices; (2) revocation of permission by an individual that affects BA's ability to use or disclose PHI; and (3) any restrictions on use or disclosure of PHI to which CE agrees and that affect BA's activities.		
Definitions: Section of BAA setting forth defined terms; provided, however, that careful review is warranted if it appears BAA is using definitions that are different than those found in HIPAA.		