
HIPAA COMPLIANCE INVENTORY: BUSINESS ASSOCIATE

The Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act") has made a number of changes to the HIPAA privacy and security rules. Under the HITECH Act, certain provisions of the privacy rule, and the entire security rule, are directly applicable to business associates.¹ As a result, business associates may be directly liable to State and Federal governments for penalties for failing to comply with those requirements. Such liability is in addition to the contractual liability the business associate has to the covered entity. To determine what actions a business associate should take to ensure it is in compliance with the HIPAA privacy and security requirements applicable to the business associate, please complete the following checklist.

- 1) Has business associate taken actions to ensure it is complying with the provisions of its business associate agreements that are required by the existing HIPAA privacy rule?² Yes No
- 2) Has business associate taken actions to ensure it is complying with the new privacy provisions added to HIPAA by the HITECH Act?³ Yes No
- 3) Have privacy policies and procedures been adopted and/or updated?⁴ Yes No
- 4) Has a security risk assessment been conducted? Yes No
- 5) Has a security officer been selected? Yes No
- 6) Have security policies and procedures been adopted? Yes No
- 7) Are updates needed to security policies and procedures in light of the HITECH Act?⁵ Yes No
- 8) Does the business associate provide its clients (i.e., covered entities) with a business associate agreement?⁶ Yes No
- 9) Has the business associate's business associate agreements been updated for the HITECH Act? Yes No

¹ Business associates are persons who, on behalf of a group health plan, either (1) perform or assist with performing an activity involving the use or disclosure of PHI, or (2) provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, if the performance of such services involves access to PHI. Business associates may include claims administrators, COBRA administrators, insurance brokers/agents, benefit consultants, benefit software vendors, etc.

² Pursuant to the HITECH Act, HHS may directly enforce these provisions against business associates. These provisions include: (1) implementing privacy safeguards, (2) ensuring subcontractors that have access to PHI agree to the terms and conditions of business associate's business associate agreements, and (3) providing information necessary to provide an accounting of PHI disclosures.

³ HHS may directly enforce the privacy provisions of the HITECH Act against business associates. Those provisions include: (1) the breach notification requirements, and (2) the restrictions on the sale of PHI and the use of PHI in marketing materials.

⁴ Technically, a business associate is not required to adopt privacy policies and procedures. Nevertheless, to ensure compliance with the provisions of the privacy rule that are directly applicable to the business associate, a business associate should consider implementing privacy policies and procedures.

⁵ The HITECH Act does not directly require changes to security policies and procedures. However, adjustments to the policies and procedures may be needed if a covered entity chooses to use encryption to make its PHI "secure" for purpose of the HITECH Act's breach notification requirements.

⁶ Historically, it has been the covered entity's responsibility to ensure it has entered a business associate agreement with each business associate. Now that the security rule is directly applicable to business associates, business associates likely have direct responsibility for complying with the security rule's business associate agreement requirement.