

## HIPAA COMPLIANCE INVENTORY: COVERED ENTITY

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. As a result, covered entities<sup>1</sup> are required to take certain actions to come into compliance with the amended law. This is also a good opportunity review the covered entity's compliance with existing HIPAA privacy and security requirements. To determine what actions an employer should take to ensure the covered entity is in compliance with all HIPAA privacy and security requirements, complete the following checklist.

- 1) Have privacy policies and procedures been adopted?  Yes  No
- 2) Have privacy policies and procedures been updated for security rule?  Yes  No
- 3) Have privacy policies and procedures been updated for the HITECH Act?  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?<sup>2</sup>  Yes  No
- 8) Has a notice of privacy practices been distributed?  Yes  No
- 9) Have plan participants been notified of the availability of the notice of privacy practices every three years?  Yes  No
- 10) Has the notice of privacy practices been updated for the HITECH Act?  Yes  No
- 11) Does the covered entity have business associates<sup>3</sup>?  Yes  No
- 12) Does the covered entity provide its business associates with a business associate agreement?<sup>4</sup>  Yes  No
- 13) Has the covered entity's business associate agreements been updated for the HITECH Act?  Yes  No

---

<sup>1</sup> For purposes of this document, a "covered entity" is a group health plan or several group health plans that are part of an organized health care arrangement. For self-insured plans, the employer sponsoring the plan(s) is generally responsible for ensuring the covered entity complies with all HIPAA's privacy and security requirements. For insured plans, if the employer takes a hands-off approach to protected health information, the insurance carrier is primarily responsible for ensuring the covered entity complies with HIPAA's privacy and security requirements.

<sup>2</sup> 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.

<sup>3</sup> A business associate is a third party that provides services with respect to the covered entity if, as a part of those services, the business associate handles, creates, or has access to protected health information.

<sup>4</sup> It is the covered entity's responsibility to ensure there is a business associate agreement with each business associate, but in practice business associates often provide business associate agreements to their clients.