COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual Resource: Business Associate Agreement Checklist and Considerations

By Emma Trivax, Erin Whaley, Jim Koenig, Brent Hoard, Jonathan Ishee, and Kimberly Gillespie.[1]

Business Associate Agreement Background

In 2013, the U.S. Department of Health & Human Services (HHS) Office for Civil Rights announced a final rule that implemented a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to further strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[2] HIPAA requires that a covered entity enter into a business associate agreement (BAA) with a business associate. Among other things, the HITECH Act made business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements. The HITECH Act was needed to strengthen the HIPAA privacy and security protections for individual's health information maintained in electronic health records and other formats.

Definitions

Including applicable definitions into a BAA will clarify language and advise the writer/reader what terms mean. BAAs may include a statement with catch-all or specific definitions, as described below.

Catch-all Definition

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions

a. **Business associate**: "Business associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. § 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

b. **Covered entity**: "Covered entity" shall generally have the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

c. **HIPAA Rules**: "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. §§ 160; 164.

d. **Breach**: This term means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under Subpart E of this part which compromises the security or privacy of the

protected health information.

e. **Unsecured protected health information**: This term means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.