Covered Entity

A covered entity is a health care provider, a health plan or a health care clearing house which, in its normal activities, creates, maintains or transmits Protected Health Information (PHI) with some exceptions. Most health care providers employed by a hospital are not covered entities. The hospital is the covered entity and responsible for implementing and enforcing HIPAA compliant policies.

Employers – despite maintaining health care information about their employees – are not generally considered covered entities unless they provide self-insured health coverage or benefits such as an Employee Assistance Program (EAP). In these cases they are considered to be “hybrid entities” and any unauthorized disclosure of PHI may still be considered a breach of HIPAA.

Business Associate

A business associate is a person or business that provides a service to – or performs a certain function or activity for – a covered entity when that service, function or activity involves the business associate having access to PHI maintained by the covered entity. Examples of Business Associates include lawyers, accountants, IT contractors, billing companies, cloud storage services, email encryption services, etc.

Before having access to PHI, the Business Associate must sign a Business Associate Agreement with the Covered Entity stating what PHI they can access, how it is to be used, and that it will be returned or destroyed once the task it is needed for is completed. While the PHI is in the Business Associate’s possession, the Business Associate has the same HIPAA compliance obligations as a Covered Entity.

HIPAA Requirements

Despite the intentionally vague HIPAA requirements, every Covered Entity and Business Associate that has access to PHI must ensure the ***technical****,* ***physical*** *and* ***administrative***safeguards are in place and adhered to, that they comply with the HIPAA Privacy Rule in order to protect the integrity of PHI, and that – should a breach of PHI occur – they follow the procedure in the HIPAA Breach Notification Rule.

All risk assessments, HIPAA-related policies and reasons why addressable safeguards have not been implemented must be chronicled in case a breach of PHI occurs and an investigation takes place to establish how the breach happened. Each of the HIPAA requirements is explained in further detail below. Businesses that are unsure of their obligation to comply with the HIPAA requirements should seek professional advice.

Retrieved on November 26, 2019 from <https://www.hipaajournal.com/hipaa-compliance-checklist/>