

HIPAA compliance:

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection. Companies that deal with protected health information (PHI) must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance

HIPAA's three compliance areas include:

1. The Privacy Rule, which restricts covered entities' and business associates' use and disclosure of an individual's PHI)
2. The Security Rule, which requires covered physician practices to implement "administrative, technical, and physical safeguards" to ensure the confidentiality, integrity, and availability of electronic
3. The Breach Notification Rule, which requires covered entities to notify affected individuals, the Secretary of the U.S. Department of Health & Human Services (HHS), and in some cases — the media when they discover a breach of a patient's unsecured

How Does HIPAA Apply to Your Company?

The level and extent of HIPAA compliance requirements vary based on whether your company is considered a "covered entity". However, even businesses not considered covered entities and those excluded from HIPAA requirements should still take basic steps to ensure the protection of employee's information.

Who and What is Excluded from HIPAA?

Any company or plan that does not meet the definition of covered entity or business associate is exempt from HIPAA rules. Exceptions include:

Employers who don't offer any HIPAA covered benefits like medical, dental, vision, or

Non-HIPAA plans like Short-term and Long-term Disability, Worker's Compensation, Life insurance, Accidental Death and Dismemberment, OSHA required testing, Auto liability insurance that contains payment for medical damages, and Stop-loss coverage

Plans with less than 50 participants that are administered and maintained solely by the employer that established the plan, no outside third-party vendor (TPA) are used in the administration of the plan

If you fall into any of these categories, you are excluded from HIPAA regulations. Document your determination of exclusion from HIPAA regulations and retain for your records.