

The ABC's of HIPAA

Partner Quick Reference Guide

DBQ
Technology.

HIPAA

The Health Insurance Portability and Accountability Act is a federal law that sets standards for protecting sensitive patient health information that Covered Entities and Business Associates must follow.

Covered Entity

Healthcare providers, health plans, and healthcare clearinghouses that transmit health information electronically. Covered entities must follow HIPAA rules to protect patient data.

Business Associate

Companies that provide services to covered entities involving access to patient information. Business associates must also comply with HIPAA rules when handling protected health information (PHI).

OCR

The Office for Civil Rights, a division of the U.S. Department of Health and Human Services (HHS) that enforces HIPAA compliance and can investigate complaints and conduct audits. They are currently in a period of random auditing.

HHS

The U.S. Department of Health and Human Services oversees healthcare-related federal agencies like OCR.

HITECH Act

The Health Information Technology for Economic and Clinical Health Act promotes the adoption of health information technology and strengthens HIPAA provisions on data privacy and security.

The ABC's of HIPAA

Partner Quick Reference Guide

NIST

The National Institute of Standards and Technology, which develops cybersecurity standards and guidelines that HIPAA covered entities must follow for data encryption.

ePHI

Electronic Protected Health Information refers to any individually identifiable health information that is created, stored, transmitted, or received in electronic form.

EMR/EHR

Electronic Health Record/Electronic Medical Record are often used interchangeably to refer to a digital record of a patient's health information, with EMRs typically limited to a single healthcare organization and EHRs designed for interoperability and data sharing across the healthcare system.

BAA

A Business Associate Agreement is a written contract between a HIPAA-covered entity and a business associate that establishes the permitted and required uses and disclosures of protected health information (PHI) by the business associate. It also outlines the safeguards that the business associate must implement to protect the privacy and security of the PHI.

Privacy Rule

One of HIPAA's 4 rules. Establishes national standards for protecting individuals' health records and other personal health information. It controls how PHI may be used and disclosed.

Security Rule

Another of HIPAA's 4 rules. Outlines administrative, physical, and technical safeguards that covered entities and business associates must implement to ensure the confidentiality, integrity, and availability of electronic PHI.