What is Protected Health Information (PHI) ?

Picus Labs
| 2 MIN READ CREATED ON August 13, 2025
What is Protected Health Information (PHI) ? PHI (Protected Health Information) refers to any individually identifiable health information that is created, stored, transmitted, or received in any form whether on paper, spoken, or digital. It is protected under the HIPAA Privacy Rule and includes health data such as medical records, patient history, billing information, and other health-related data that can be linked to a specific individual. While ePHI (Electronic Protected Health Information) focuses on the digital version of this data, PHI includes all forms, and its protection spans across both digital and non-digital formats. Examples of PHI: Common examples of PHI include: Lab results on paper records or EHRs A patient s insurance form submitted verbally or via encrypted email Diagnoses and prescriptions documented in paper charts or digital systems Billing information in paper form or
cloud-based systems Scheduling data in paper records or digital platforms Each of these types of data, when tied to an individual, qualifies as PHI. Whether handled in digital, paper, or spoken form, they are subject to HIPAA's Privacy and Security Rules. PHI vs. ePHI: What s the Difference? PHI (Protected Health Information) ePHI (Electronic PHI) Can exist in paper, verbal, or digital form Exists only in electronic form Covered by the HIPAA Privacy Rule Covered by both Privacy and Security Rules Requires physical and administrative safeguards Requires physical, administrative, and technical safeguards The key distinction is that ePHI requires additional technical safeguards like encryption, access management, and audit logging while PHI, regardless of its form, is primarily subject to privacy rules. Why PHI Matters for HIPAA Compliance PHI, regardless of whether it's in digital, paper, or verbal form, must be secured to prevent unauthorized access and disclosure. HIPAA-covered entities are legally required to protect the confidentiality, integrity, and availability of PHI, both digitally and physically. Non-compliance can lead to regulatory penalties, reputational damage, and
breach notifications.
How to Protect PHI To properly protect PHI and comply with HIPAA, organizations must implement a multi-layered defense strategy that

includes: Role-based access

control

Secure data transmission and encrypted storage Regular risk and vulnerability assessments Audit logging and activity monitoring Continuous testing of security

control

effectiveness Although PHI in paper form needs protection, ePHI s additional risks and technical requirements mean that healthcare organizations must prioritize safeguarding digital PHI against evolving cyber threats. Need to validate your HIPAA safeguards? Picus Security helps healthcare organizations continuously test and validate the effectiveness of security controls that protect PHI, ensuring HIPAA compliance Explore HIPAA Compliance with Picus