HIPAA's Three Rules Explained

Privacy, Security, and Breach Notification

Privacy Rule:
Protects Patient Information (PHI)

01 It defines how Protected Health Information (PHI) can be used or disclosed.

02 It applies to healthcare providers, insurers, and partners.

03 It gives patients' rights to access their records, request corrections, and control disclosures.

Aim: To keep patient data confidential and in the right hands

Security Rule:
Safeguards electronic PHI (ePHI)

01 It applies only to digital health data.

02 It requires 3 types of safeguards: Administrative, Physical, and Technical.

Aim: To ensure data is secure from breaches and unauthorized access

Breach Notification Rule:
Transparency after a data breach

01 It requires notification if PHI is compromised

02 It notifies affected individuals, government authorities, and media (if large-scale breach)

03 Timeline: Within 60 days of discovery

Aim: To ensure accountability and timely response

At a Glance

Rule	What It Covers	Key Outcome
Privacy Rule	Use & disclosure of PHI	Patient control & confidentiality
Security Rule	Protection of ePHI	Data security & risk management
Breach Notification Rule	**Response to data breaches**	**Transparency & accountability**

Strengthen your HIPAA compliance beyond the basics.

Schedule a quick readiness consultation with Ampcus Cyber to identify gaps in your Privacy, Security, and Breach Notification controls.