RCMEASY GUIDE

HIPAA, BAAs & Data Security: What to Ask Any Billing Partner

Compliance doesn't disappear when you outsource — it's shared.

What a BAA Actually Covers

A Business Associate Agreement defines how a vendor handling Protected Health Information (PHI) on a provider's behalf is required to protect it. It's a legal requirement, not a marketing checkbox — every vendor touching PHI should sign one without hesitation, and be able to explain what it covers.

Questions to Ask About PHI Access

Who on the vendor's team can actually see PHI, and is that access limited to the people working your account specifically? Is PHI encrypted both at rest and in transit? What is the vendor's breach-notification process, and how quickly are you notified if something goes wrong?

Red Flags

Vendors who are vague about their BAA, who can't describe specific safeguards beyond "we're HIPAA compliant," or who can't explain how access is limited internally are worth a second look before signing anything. Specificity is the difference between a real compliance posture and a marketing claim.

How RCMEasy Approaches This

PHI handling for every RCMEasy client is governed by a signed Business Associate Agreement — not just a badge on a webpage. Access is limited to the team working that account, with reasonable administrative, technical, and physical safeguards applied consistently to protect all PHI handled on a client's behalf.

NEXT STEP

See Our Security & Compliance Page

rcmeasy.com · A Guide by RCMEasy