Business Associate Agreement (BAA)

Protected Health Information (PHI) includes any patient name, mailing address, e-mail address, phone number, SS#, and any other information that could be used to identify a patient.

Risk Areas	Patient Billing Detail	Accounts Receivable Detail	Write-offs to Doubtful Accounts	General Ledger	Journal Entries
De-identifying Tactics	Use summaries only. If detail needed, ask client to delete identifiers or replace with patient account numbers.			Delete identifiers or replace with patient account numbers.	

- Only sign a BAA IF access to PHI is required to complete the engagement. Don't sign as "insurance" for client in case they inadvertently provide you with PHI. The BAA shifts liability for protecting patient privacy to you. Unless you explicitly agree to access PHI for a specific purpose, the liability should reside with the client.
- If you're not 100% certain your electronic systems comply with the HIPAA Security Rule, ask client to specify in the BAA that you will ONLY receive printed copies and you will NOT convert them to electronic format.
- If you determine that electronic access to PHI is necessary for your engagement, remember that ANY cloud-based software or data storage provider that you will use to process, transmit or store the e-PHI will also need to sign a BAA.