

HIPAA and Vendor Compliance

As if managing your own HIPAA compliance wasn't complicated enough, did you know your organization is responsible for ensuring vendor compliance? You need to be collecting information from your business associates to show how privacy and security are being monitored. If you are ever audited or breached, an investigator will ask questions such as:

- Do you know the names and contact information for your business associates?
- Do you know if your business associates subcontract? And if they do, what limitations are imposed to protect your PHI? Do they have BAAs in place with their subcontractors? And do they monitor the compliance efforts of those subcontractors?
- Do you address any identified risks/vulnerabilities/threats discovered or known involving your business associates and their subcontractors?
- How often are you reviewing the compliance efforts of your business associates and their subcontractors?
- Do you require your business associates to provide proof of a risk analysis or internal audit or compliance?

Wouldn't it be nice if it were as simple as signing the Business Associate Agreement? As much as we would love to believe that our responsibility with our business associates ends at the signing of a Business Associate Agreement, that is simply not true.

Sarah Badahman

HIPAAtrek

sarah@hipaatrek.com