



next I.T.

Tips For Drafting A Comprehensive HIPAA Business Associate Agreement

This checklist will help you to craft a BAA that covers all of the necessary bases, follows the language guidelines set by HIPAA standards, and meets the minimum requirements for compliance.



Business Associate Agreements (BAAs) are an important part of HIPAA compliance for your practice. These contracts should clearly outline a Business Associate's responsibilities regarding your PHI and can pose a serious liability risk if the BAA isn't negotiated effectively. Any outside entity or individual that is charged with receiving, maintaining, creating, or transmitting PHI is considered a Business Associate and needs to have a BAA of their own in place with your practice.

This checklist will help you to craft a BAA that covers all of the necessary bases, follows the language guidelines set by HIPAA standards, and meets the minimum requirements for compliance.

Your BAA should require a Business Associate to:

- Have appropriate safeguards in place and take any necessary steps to comply with the provisions of the Security Rule where applicable to your circumstances
- Have a process in place to notify you of any unauthorized use or disclosure of PHI that the Business Associate becomes aware of, including breaches of unsecured PHI and security incidents
- Take steps to ensure that any subcontractors employed by the Business Associate to receive, maintain, create, or transmit PHI on the Business Associate's behalf are in agreement with and will be held to the same restrictions and conditions as the Business Associate
- Provide ready availability of PHI to individuals with certain rights (access, amendment, accounting, etc.)
- Have their internal practices and records relating to the use and disclosure of any and all PHI made available to the Secretary of the Department of Health and Human Services (HHS) for the purpose of determining your practice's HIPAA compliance
- Agree to clear terms regarding the return or destruction of all PHI if the BAA is terminated. If PHI cannot be returned or destroyed for any reason, the Business Associate must agree to extend the protections offered by the BAA and limit any further uses and disclosures of the PHI in question

The nuances of a BAA can differ from Business Associate to Business Associate, and depend largely on the needs of your practice. Compliance guidelines are steadfast, but how you go about meeting those requirements is for the most part up to your discretion.





Contact us for any questions you have regarding HIPAA compliance and security.

Call or email us at

1 866.388.6398 or **sales@next-it.net**