OnceHub Support

The OnceHub BAA

Last Modified on Jan 14, 2021

The OnceHub Business Associate Agreement (BAA) is a legal mechanism for ensuring patient data is adequately protected. To be HIPAA compliant, covered entities must sign a BAA with their business associates. The OnceHub standard BAA is available to eligible account holders (accounts with at least four Users) at no additional cost. View our Business Associate Agreements

What are my responsibilities?

To comply with the terms of the OnceHub BAA, account holders must use our service in a HIPAA compliant manner. For example, you should enable account security policies to satisfy the requirements of the HIPAA security rule. Users that are not familiar with the HIPAA security rule should follow best practices when securing their OnceHub account. Learn more about securing your account

What is covered?

The OnceHub BAA covers patient data that is stored on our servers. Data that is passed to third-parties via integrations is outside our control and not covered by the BAA. If you are using third-party integrations you should ensure that the receiving party is compliant with HIPAA. For example, if you have a calendar integration with Google, you should make sure that your BAA with Google covers the data transferred from OnceHub.

SMS notifications are not covered by the OnceHub BAA. The SMS service is not HIPAA compliant and should only be used to send ScheduleOnce booking notifications that do not contain patient information.

The OnceHub help desk software is not HIPAA compliant. Support inquiries containing health information should not be sent to the OnceHub support team.

Why can’t I downgrade?

A HIPAA compliant account cannot be reverted to a regular OnceHub account. Patient data is stored for the lifetime of your account, and your patient data is regulated by HIPAA until it is deleted. Patient data stored in OnceHub is only deleted when you stop using our service.

HIPAA compliant accounts require additional security controls. For example, Short session timeouts should be enabled to satisfy the HIPAA security rule. HIPAA compliant accounts must use these security features and can’t be downgraded to a lower plan.