Nightfall™

Guide to HIPAA Compliance for SaaS Applications

Section A - Evaluating a provider's status as a Business Associate

1. Evaluating the Service Provider's Status as a HIPAA Compliant Entity

□ **The service provider is capable of executing a Business Associate Agreement (BAA)**

Vendors or service providers whose work requires them to handle PHI for a HIPAA covered entity must be able to sign and execute a BAA. Even if the provider's platform does support the requirements necessary for satisfying HIPAA, the BAA must be in effect before your organization can be in compliance with HIPAA. Often a provider's terms of service may clarify if and how the entity can execute a BAA.

□ **The service provider can satisfy your specific HIPAA use case**

Before executing a BAA, confirm with the provider that your specific HIPAA use case can be satisfied using their service. For example, a service like Slack is not sanctioned for communication between patients and healthcare providers but is suited for communication between providers. An organization seeking to use Slack to communicate with patients would not have an appropriate use case, even though the application serves other HIPAA compliant use cases.

Section B - Evaluating proper implementation of security controls

2. Implementing HIPAA Security Rule Technical Safeguards

□ **Adopt the appropriate product or tier of service**

SaaS applications can offer a variety of service tiers, however, not all of them may allow for the configurations or controls needed to maintain HIPAA compliance while using the application. Ensure that your organization purchases the tier or product(s) required for HIPAA compliance.

□ **Successfully implement the appropriate audit controls**

HIPAA covered entities leveraging digital technologies for sharing and storing ePHI must have mechanisms to record and examine access and other activities within systems that contain or use ePHI. Such mechanisms may be offered by the service provider or through marketplaces managed by the service provider. These can include (but are not limited to):

- Audit Logs
- Security Information and Event Management (SIEM)
- Data Loss Prevention (DLP)

□ **Ensure administrative and physical safeguards are in place**

The above items ensure your organization is compliant with the HIPAA Security Rule technical safeguards for ePHI. Beyond the HIPAA Security Rule technical safeguards, implementing facility and device level policies are essential. Make sure these are in place regardless of whether you adopt SaaS applications. Learn more here.

□ **Successfully implement the appropriate access controls**

HIPAA covered entities leveraging digital technologies for sharing and storing ePHI must have policies and solutions in place that limit access exclusively to authorized persons. Such solutions may be offered by the service provider or through marketplaces managed by the service provider. These can include (but are not limited to):

- Single Sign-on (SSO)
- Multi-factor Authentication (MFA)
- Data Loss Prevention (DLP)

□ **Successfully implement the appropriate integrity controls and ensure transmission security**

HIPAA covered entities leveraging digital technologies for sharing and storing ePHI must have policies and solutions in place that ensure ePHI isn't improperly altered or destroyed. Such solutions may be offered by the service provider or through marketplaces managed by the service provider. These can include (but are not limited to):

- Encryption at rest
- Encryption in transit
- Backup/Archival

Disclaimer: While we have made every attempt to ensure that the information contained in this guide is accurate to our best efforts, Shoreline Labs, Inc., is not responsible for any errors or omissions, or for any result obtained from the use of this information. This guide is based on a specific point in time, and is no guarantee of completeness, accuracy, timeliness, or of the results obtained from the use of this information. Nothing in this guide should be used as a substitute for the independent investigations and the sound technical and business judgment of your legal and compliance professionals. We do not accept any liability if this guide is used for an alternative purpose from which it is intended, nor to any third party for any purpose. In no event will Shoreline Labs, Inc., its employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on this guide or for any consequential, special or similar damages, even if advised of the possibility of such damages.