HIPAA Compliance Datasheet

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a United States federal law requiring the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.[1]

The general rules of HIPAA for covered entities and their business associates are to:

1. Ensure the confidentiality, integrity, and availability of all Protected Health Information (PHI) they create, receive, maintain or transmit
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information
3. Protect against reasonably anticipated, impermissible uses or disclosures
4. Ensure compliance by their workforce

Asana's Commitment to Covered Entities & Business Associates

Businesses that are subject to the Health Insurance Portability and Accountability Act of 1996 can use Asana to support HIPAA-compliant work management.

Asana views security and compliance as a shared responsibility between Asana and the customer. It is Asana's responsibility to empower customers with services they need to maintain HIPAA compliance. It is the customer's responsibility to ensure their Asana domain is architected to support HIPAA compliance.

Customers have an independent obligation to maintain compliance with the applicable requirements under HIPAA and HITECH by implementing appropriate administrative, technical, and physical safeguards to protect PHI hosted and processed by Asana. Asana has put in place security and compliance controls for all customer data, including Asana customers who are subject to HIPAA. We each commit to those obligations and responsibilities in the Business Associate Addendum between Asana and Customer.

[1] Center for Disease Control & Prevention, Public Health Law

Please note Asana has not yet been evaluated to ensure compliance with other global healthcare laws and regulations. This guide only applies for HIPAA compliance.

Enabling HIPAA Compliance in Asana

Customers must execute Asana's Business Associate Agreement (BAA) if they are subject to HIPAA and intend to store Protected Health Information (PHI) in their Asana domain. Customers retain the primary responsibility for ensuring compliance with HIPAA. Asana will satisfy its obligations as a Business Associate primarily by empowering customers with the necessary tools to maintain HIPAA compliance.

Executing Asana's Business Associate Agreement

To execute Asana's Business Associate Agreement and activate HIPAA compliance for Asana:

1. Customers will first need to purchase HIPAA compliance for Asana, which is available only with an Enterprise plan for the full organization. To purchase **Asana Enterprise** and HIPAA compliance for Asana, please **contact our sales team**.
2. Once HIPAA compliance has been purchased and provisioned, an **Asana Super Admin** will need to review and execute the Business Associate Agreement and the HIPAA Use Requirements in Asana's Admin Console.
3. Users will need to allow 24 hours between signing the BAA and Use Requirements for HIPAA compliance to activate across their organization.
   a. Upon signature, the Super Admin is responsible for reviewing any existing app. Authorizations via the Apps tab in the Admin Console. Customers are solely responsible for reviewing the security of any third party integrations on their own, including entering into separate Business Associate Agreements or any other data protection terms with these service providers if necessary. Asana does not have Business Associate Agreements with all third parties that may integrate with Asana.

Upon confirmation, Asana will adjust several product features in order to provide customers with a product experience that prioritizes security and privacy by default.[2]

Please note once HIPAA compliance is enabled in Asana, reverting to a version of Asana without HIPAA Compliance will require domain deletion. If HIPAA functionality is removed from a domain, Asana is required to proceed with domain deletion in order to preserve the confidentiality of data. The Asana Admin Console offers Asana admins a way to export their organization's data as a JSON file.[3]

[2] In most cases, these product changes are overridable by an organization's Super Admin. However, overriding Asana's defaults may impact an organization's HIPAA compliance. We leave it up to the customer to make these determinations with relevant legal and compliance teams in their organization

[3] Please see the **Asana Help Guide** for more details on how to export data in Asana.

How Asana Supports HIPAA Compliance

The following table demonstrates how Asana supports HIPAA compliance in accordance with HIPAA Security and Privacy Rules.

Table Key
* = Feature cannot be overridden by Super Admin

HIPAA Standard	How Asana Meets the Standard
Access Control	
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to authorized persons or software programs.	● Most email notifications will be turned off by default. Individual users of Asana cannot opt-in to receive emails from Asana regarding tasks, projects, goals, or any other Asana features.* ● Read-only links will be disabled for logged out users. ● Mobile push notifications will not include task information.* ● Attachments cannot be previewed or shared on mobile.* ● All projects, portfolios, teams, and goals will be set to private by default.* ● Asana's native Vimeo video integration will be disabled by default. ● All integrations and Personal Access Tokens (PATs) within an Asana domain will be disabled by default. ○ Previously enabled apps will remain enabled. New applications will require an Asana Admin's approval in order to be enabled. ○ Customers are solely responsible for reviewing the security of any third party integrations on their own, including entering into separate Business Associate Agreements or any other data protection terms with these service providers if necessary. Asana does not have Business Associate Agreements with all third parties that

	may integrate with Asana.
Unique User Identification	
Assign a unique name and/or number for identifying and tracking user identity.	● MFA will be required for all domain members and guests by default. ● Enterprise admins can configure their identity provider and request their users to log in to Asana using their cloud IdP account credentials. ● “Password Strength” in Asana’s Admin Console will be set to “Strong” by default (must have at least 8 characters and must include characters from at least three of the following types: lowercase, uppercase, numbers, and special characters).
Automatic Logoff	
Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	● On Asana web and desktop, a forced logoff for all users after 14 days will be applied by default. ● On Asana mobile (iOS and Android[4]), a forced reauthentication for all users after 14 days will be applied by default.*
Audit Controls	
Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	● In order to monitor for unusual activity, such as logins, it is highly recommended that customers use Asana’s Audit Log API.[5] ● Customers can use Asana's export functionality or APIs to monitor for policy violations.
Integrity & Integrity Mechanism	
Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. *Implement electronic mechanisms to corroborate that electronic protected*	● All projects, portfolios, goals, and teams in Asana will be set to private by default.* ● Asana’s Audit Log API provides Admins in Enterprise organizations access to an immutable log of key events across their organization. Using the Audit Log API, Super Admins can capture and act upon important

[4] Users in HIPAA domains may use Asana iOS 9.29.0 or later and Asana Android 7.20.0 or later to help support HIPAA compliance

[5] For more, see **Audit Log API**

health information has not been altered or destroyed in an unauthorized manner. *Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.*	security and compliance related changes. ● Asana stores audit logs for 90 days from the date of capture. Those who would like a longer retention period may choose to use their SIEM or another storage solution for continuous log ingestion.
Person or Entity Authentication	
Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	● 2FA will be required for all domain members and guests by default. ● “Guest invites” control will be set to “Admins only” by default. ● “Password Strength” in Asana’s Admin Console will be set to “Strong” by default (must have at least 8 characters and must include characters from at least three of the following types: lowercase, uppercase, numbers, and special characters).
Transmission Security	
Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. *Implement a mechanism to encrypt and decrypt electronic protected health information.*	● For all customers, customer data is encrypted with AES 256-bit encryption at rest. ● Connections to app.asana.com are encrypted with 128-bit encryption and supports TLS 1.2 and above. Connections are encrypted and authenticated using AES_128_GCM and use ECDHE_RSA as the key exchange mechanism. ● Asana supports forward secrecy and AES-GCM, and prohibits insecure connections using RC4 or SSL 3.0 and below. ● Logins and sensitive data transfers are performed over encrypted channels (TLS) only.
Data Retention and Disposal	
Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	● Tasks that are deleted in Asana will remain in the “Deleted Items” for 30 days, then will be permanently deleted. ● Projects that are deleted in Asana are recoverable for 7 days. Tasks within projects that are deleted follow standard task deletion behavior where they remain in

	“Deleted Items” for 30 days, then are permanently deleted. ● Customers who would like to create longer retention policies can export data from Asana to customize the retention policy. ● If HIPAA functionality is removed from a domain, Asana is required to proceed with domain deletion in order to preserve the confidentiality of data. Domain deletion will occur 90 days after cancellation.[6]

Additional Product Use Considerations

- PHI storage should be limited to project or task descriptions, task titles, custom fields on tasks, comments, and attachments on tasks.
- Asana is not an EHR (Electronic Health Record). Asana does not maintain the designated record set and should not be the system of record for health information. Customers may not create Asana accounts in their domain for their patients, patient family members, plan members, or any other external parties to communicate.
- When contacting Asana User Operations, you should not provide PHI to UO in any support tickets. Please do not share PHI when on calls with Asana representatives.

Privacy, Certifications, and Compliance

Asana makes an ongoing commitment to ensure our services meet global requirements for security, privacy, and compliance. To learn more about Asana’s current certifications and attestations, please visit our **Trust page**.

Further Reading

Asana Security and Privacy Whitepaper

[6] Policies may be different for customers accessing the Asana Smiles for Align tier. For customers accessing the HIPAA Smiles tier, please consult your agreements with Asana.