

HIPAA-Compliant Collaboration with Slack



Configure Enterprise Grid to be your HIPAA-compliant collaboration hub

At Slack, we are committed to ensuring the data you share is always protected.

Slack complies with many broadly recognized standards and offers tools to help customers meet their compliance requirements. Companies that are subject to HIPAA (Health Insurance Portability and Accountability Act of 1996) such as health plans,

health care providers, health insurance companies, health benefit providers, and the many businesses that provide them with services, can configure Slack Enterprise Grid to support HIPAA-compliant collaboration. When Slack is helping these customers carry out healthcare activities or functions, Slack is a vendor/service provider classified as a business associate (BA) under HIPAA.

BENEFITS

Share protected health information confidently

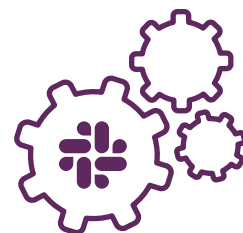
Enterprise Grid is Slack's solution for large, complex organizations. It includes all of the security and governance functionality you expect in an enterprise solution but with an intuitive, consumer-like experience that results in a high rate of adoption.

When configured and used according to Slack's specific requirements for HIPAA entities, teams collaborating on Enterprise Grid can share Protected Health Information (PHI) within direct, group and channel messaging, and in file uploads.



Control your company's use of Slack

Compliance monitoring is not one-size-fits-all. Slack Enterprise Grid provides APIs to support monitoring of access, activity, and data in customer workspaces. This ensures that every company can implement tools and processes that are right for them. You can use Slack's Discovery APIs and set up an external Data Loss Prevention (DLP) provider to enforce message and file restrictions and export message and file content for HIPAA compliance.



Slack partners with many best-of-breed providers that may already be present in your company.

Audit Logs

Partner enabled functionality:

- Download logs of activity within your Slack workspaces
- Captures events like file downloads, file uploads, admin setting changes



Data Loss Prevention

- API-based with pre-built connectors to leading solution partners

Partner enabled functionality:

- Monitor messages and files in public channels, private channels and direct messages
- Integrated DLP solutions have complete access to all content within your enterprise organization
- Actively quarantine and remove non-compliant content in near real-time



WHAT YOU SHOULD KNOW ABOUT USING SLACK IN A HIPAA-REGULATED ENVIRONMENT

Slack Plan Supported: Enterprise Grid

- **Requirements:** Contact Slack to get the Slack Requirements for HIPAA Entities guide
- **Other tools you will need:** DLP solution, SSO solution, backup/archival
- **Process:**
 - Review and commit to implementing the Slack Requirements for HIPAA Entities guide.
 - Sign Slack’s business associate agreement (BAA)
 - Provide Slack with a list of all Slack orgs or workspaces with which you plan to use PHI

MORE ON SLACK REQUIREMENTS FOR HIPAA ENTITIES

- The *Slack Requirements for HIPAA Entities* guide is the only comprehensive source of implementation requirements.
- Slack may not be used to communicate with patients, plan members, or their families or employers. Patients, plan members, and their families or employers may not be added as users or guests to any Slack workspaces or channels.
- While users may discuss Protected Health Information in message content and upload files that contain PHI, users may not include PHI in some specific fields.
- There are restrictions on using email forwarding and ingestion with Slack if transmitting PHI over email.
- There are controls needed if using shared channels to communicate between two separate companies or workspaces.
- Channels in which PHI may be shared through messages or documents should be set as private.
- You must inform your users about how to use and configure Slack so it can be used in compliant ways. You can do so by using various available Slack capabilities such as custom terms of service, customizable bots, mandatory org-wide channels, pinned posts and PHI deletion notifications.
- There are special considerations for devices, adding users, patient home visits and other situations.