Dropbox Business

Getting started with HIPAA

Dropbox Business best practices

Dropbox Business customers subject to laws like the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) should take special care to make sure their use is consistent with legal requirements. To help aid in your compliance efforts, we've put together a few recommended best practices that you should consider when configuring your accounts.

Configure sharing permissions

Dropbox Business gives you flexibility to determine your team's sharing needs. If your team handles Protected Health Information (PHI), you can configure your account so folders, links, and Paper docs can't be shared with people outside of your team. When team members create shared folders, they can further customize the folders' settings and choose the appropriate level of access — edit or view-only.

Strengthen authentication

- **Two-step verification** Team admins can require members use two-step verification to sign in to their accounts. This highly recommended security feature adds an extra layer of protection to users' Dropbox accounts. Once enabled, Dropbox will require a six-digit security code in addition to a password upon sign-in or when linking a new computer, phone, or tablet.
- **SSO** If your company already manages password policies and authentication with a central identity provider, you may want to set up single sign-on for your Dropbox Business team. By using your existing SSO provider, your team members don't have to remember yet another password. More importantly, authenticating access to Dropbox will be managed using the same password policies as other services at your company.

Disable permanent deletions

By default, the person who uploads a file or the owner of a shared folder or Paper doc can perform permanent deletions in Dropbox. To help customers adhere to their retention requirements, we recommend admins disable the "Permanent Delete" feature from the Admin Console. By turning off this feature, you can limit the ability to permanently delete content (both files and Paper docs) to team admins only.

Dropbox Business

Getting started with HIPAA

Conduct regular access reviews

- **Team members** Team members can be easily added, removed, and reviewed from the Admin Console. To ensure sensitive data in your Dropbox Business account can only be accessed by appropriate people, we recommend frequently reviewing this list. You can then remove access when someone leaves your organization or no longer requires access due to a change in job role.
- **Devices** You and your team members should frequently review devices linked to your account and remove unused or unauthorized devices. Devices can be unlinked by both team members and the team admin. When unlinking a device, you'll also have the option to remotely wipe Dropbox content from it. Unlinking and wiping devices can keep your data secure in the event of a lost or stolen device, or if someone is leaving your team.

Monitor for unusual activity

As a team admin, you can view and export reports that detail your team's sharing, authentication, and administrator activities. We recommend that you review these activity reports to keep an eye out for any unusual activity and help keep your team secure.

Evaluate third-party apps

There is a robust ecosystem of third-party apps that you can link to your Dropbox Business account to gain added functionality. Integrations that provide services such as SIEM, DLP, and identity management can be powerful tools in strengthening your existing security practices. While these third-party apps and integrations can be great complements to your account, it's important to remember that they're not part of our included services. Therefore, they're not covered by your Dropbox terms of use, including a BAA that you might sign with Dropbox. You're responsible for evaluating these apps to determine if using them is consistent with your legal and regulatory requirements. Keep in mind that some apps link to individual accounts, while others can be linked by an admin to your entire team.

Learn about our practices

Determining if Dropbox is the right fit for your company and its regulatory needs is an important process. We encourage you to take the time to validate our practices, as you would with any other application. To give you the tools you need to verify our security practices, our ISO 27001, ISO 27018, and ISO 22301 certificates, SOC 3 assurance report, and CSA STAR questionnaire are available online. We can also provide access to additional documentation under a non-disclosure agreement to help you make an informed decision. This includes our SOC 1 and SOC 2 audit reports, CSA STAR and HIPAA assurance reports, and a mapping of our internal practices and recommendations for customers who are looking to meet the HIPAA/HITECH Security and Privacy Rule requirements.

Learn more by visiting the Dropbox Trust Guide at www.dropbox.com/business/trust. Current Dropbox Business team admins can sign a BAA electronically from the Account page in the Admin Console.

To learn more about purchasing Dropbox Business, contact our sales team at sales@dropbox.com.