

Progress ShareFile with HIPAA Support

September 2026

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Health Information Technology for Economic and Clinical Health Act (2009) are U.S. federal laws that establish and enforce national standards for Protected Health Information (PHI).

ShareFile is already built with [enterprise-grade security](#). When HIPAA support is enabled, ShareFile provides configurations and tools designed specifically to assist customers with their enhanced obligations. These features are not intended to replace your organization's broader HIPAA compliance program, and as such they do not alone guarantee HIPAA compliance. ShareFile is a configurable platform, and your organization ultimately determines how to use it. It is your responsibility to do so in a manner that complies with applicable law. You should regularly review user permissions and workflow configurations to help ensure they meet your requirements.

HIPAA support is available with select plans and only under a valid, mutually executed Business Associate Agreement (BAA) with Progress. Under the BAA, Progress is a "Business Associate" or "Subcontractor" of our customer, who is typically a "Covered Entity" or Business Associate.

ShareFile with HIPAA support is provided on a go-forward basis, starting when HIPAA support is enabled on your account and the Progress BAA is mutually executed. PHI processed before that point is not retroactively covered under HIPAA support or the Progress BAA.

ShareFile Supports HIPAA Compliance

Here's a growing list of ways that ShareFile supports your compliance efforts:

- ✓ **Business Associate Agreement.** We provide a [BAA](#) to eligible customers, ensuring that we contractually comply with our HIPAA obligations. We also require that our vendors sign BAAs to ensure that they are obligated to uphold their HIPAA obligations.
- ✓ **Limited Access.** Our vendors undergo rigorous vetting. Additionally, where appropriate, we use safeguards to limit data sharing such as using on-prem deployments or vendors that support no-view architectures (where data remains encrypted and inaccessible to them).
- ✓ **In-Product Tooltips and Reminders.**  Icons like this appear in certain areas of ShareFile's platform to signal actions that require your extra attention to best practices. Clicking or hovering over the icon may reveal tips that guide informed decisions when sharing data or adjusting account settings.
- ✓ **Dedicated Storage.** Primary data is stored in clusters specifically designed to meet HIPAA requirements.
- ✓ **Safe Email Notifications.** Generally, standard email is not HIPAA compliant. ShareFile helps reduce risk by automatically limiting the inclusion of potentially sensitive data fields (such as file names) in certain email notifications. However, ShareFile cannot control all user actions. You are responsible for ensuring that ShareFile is not used to enable the transmission of PHI in email or the transfer PHI to any email service.
- ✓ **Encrypted Inbox Messaging.** You can securely share information using encrypted email links, enabling recipients to access content directly within the ShareFile platform. This approach keeps data in a protected environment and prevents exposure through traditional, non-compliant email channels.
- ✓ **Specialized Configurations.** ShareFile continually evaluates and refines default configurations to support HIPAA requirements, reducing the need for manual adjustments. These include various restrictions on access and sharing, all designed to help minimize the risk of accidental data exposure. While many features benefit from these proactive safeguards, customers remain responsible for configuring ShareFile settings appropriately.
- ✓ **Extended Retention.** We retain event logs for extended periods to facilitate investigations.
- ✓ **Administrator-Controlled Settings.** Admins have control over various user permissions to help support your compliance policies.
- ✓ **Audits.** We undergo regular assessments by third parties to verify our HIPAA posture.
- ✓ **Avoid Conflicting Regulations.** Safeguards are built in to help avoid user enablement of features that may conflict with HIPAA.
- ✓ **Restricted Plan Changes.** Once an account is enabled with HIPAA support, it cannot be switched to a ShareFile plan that does not have HIPAA support. This helps protect PHI and ensures continuity for long-term customers, even when administrators change.

Eligible Services and Features

The following services are eligible for ShareFile with HIPAA support to the extent PHI is processed by ShareFile within the Progress-managed environment. HIPAA support does not apply to Ineligible Services and Features (such as on-prem versions of otherwise eligible services) or to otherwise eligible services that you use for Prohibited Activities (such as publicly sharing PHI), as outlined below.

- ✓ File storage and processing
- ✓ File viewing
- ✓ File co-authoring
- ✓ Audit logging and reporting
- ✓ Workflows (e.g., requests, e-signature)

Ineligible Services and Features

You may have access to services and features that involve components or workflows outside of ShareFile's control or otherwise increase the risk of unauthorized access to PHI. These items are not eligible for ShareFile HIPAA support and are not covered by a BAA with Progress. Use them with caution and at your own risk.

- **Public or anonymous sharing** that anyone can access without logging in [\[settings\]](#)
- **Public or anonymous requests** that anyone can access without logging in [\[settings\]](#)
- **Third party products**
- **Environments and services outside of the Progress-managed environment (e.g., customer's local device storage, customer-hosted or customer-managed services such as "on-prem" storage zones)¹**
- **Export capabilities that move PHI out of the Progress-managed environment** such as [Integrations](#), [connectors](#), or SIEM data export feeds.
- **ShareFile mobile apps**, such as those available on iOS or Android
- [Question and Answer](#), [Feedback and Approval](#)
- **Email**
- **Beta products, tech previews, or similar evaluation-only features**

¹ For example, although certain ShareFile apps or plugins (such as [ShareFile for Windows](#) or [ShareFile for Outlook](#)) are eligible for ShareFile with HIPAA support, the external environments they may connect to or operate in are not covered under HIPAA support.

Prohibited Activities

Customers on ShareFile HIPAA support plans must abide by the following restrictions. These are designed to reduce the risk of inadvertent PHI disclosure, particularly through systems or channels that are not eligible for ShareFile with HIPAA support or not covered under a BAA with Progress.

- ✘ Do not share PHI publicly or in any unauthorized manner.
- ✘ Do not enter PHI in any documents or fields that may be sent via email or transferred to any email service.
- ✘ Do not include PHI in any file names that may be sent via email or transferred to any email service, such as when using [ShareFile for Outlook](#), [ShareFile for Google Workspace](#), or otherwise. *Note: [Configure](#) ShareFile for Outlook to use “Text Links” instead of “Banners” to ensure that document links do not display file names.*
- ✘ Do not enter health information in fields meant for other data (e.g. date or address field).
- ✘ Do not enable or trigger folder email notifications (download alerts, upload alerts, or “notify added users” when adding people to a folder named with PHI). [\[settings\]](#)
- ✘ Do not attach completed e-signatures PDFs containing PHI to emails. [\[settings\]](#)
- ✘ Do not create hyperlinks to external environments outside of the ShareFile web app.
- ✘ Do not enter PHI in [Document Templates](#) or similar reusable multi-recipient features.
- ✘ Do not enter PHI in any public area or website. PHI may only be input into the ShareFile web app after authorized user login.
- ✘ Do not violate HIPAA or use ShareFile in any manner that causes Progress to do so.