Progress ShareFile

Progress ShareFile with HIPAA Support

March 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 continue to meet your organization's 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 another 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. Data 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**.  This icon appears 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.
- ✓ **HIPAA-Dedicated Storage**. Primary data is stored in clusters specifically designed to meet HIPAA requirements.
- ✓ **Secure 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.
- ✓ **Default Configurations**. ShareFile's default configurations are optimized for HIPAA support, reducing the need for manual adjustments. These include built-in **Multi-Factor Authentication (MFA)**, our **AI-Powered Secure Share Recommender**, as well as various restrictions on public sharing and third-party integrations, all designed to help minimize the risk of accidental data exposure. However, because admins and users can adjust settings, you must periodically review them and make updates as needed.
- ✓ **Extended Retention**. We retain event logs for extended periods to facilitate investigations.
- ✓ **Administrator-Controlled Settings**. Admins have granular control over various user permissions to help support your organizational 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 include HIPAA support. This helps protect PHI and ensures continuity for long-term customers, even when administrators change.

Ineligible Services and Features

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

- **Public or anonymous share links** (can be viewed by anyone without signing in)
- **Third party products**
- **External or customer-controlled environments outside of the ShareFile web app**
  Although ShareFile apps or plugins (such as ShareFile for Windows or ShareFile for Outlook) are HIPAA-supported, the customer-managed environments they may connect to as part of normal operation (such as third-party email systems, or your local device, on-prem, or customer-managed storage zones) are external to ShareFile and are not covered under HIPAA support.
- **Export capabilities that move PHI out of the ShareFile web app**
  Integrations and connectors are HIPAA-supported when used only to import PHI into the ShareFile web app. When these features are used to export PHI, the external destination environments are not part of ShareFile and are not covered under HIPAA support.
- **ShareFile mobile apps**, such as those available on iOS or Android
- **Question and Answer, Feedback and Approval**
- **Beta products, tech previews, or similar evaluation-only features**

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 covered under the Progress BAA.

- ✘ Do not publicly share PHI.
- ✘ 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).
- ✘ Do not attach completed PDFs in email for completed e-signature requests containing PHI.
- ✘ Do not create hyperlinks that lead 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.