box

Box and HIPAA compliance

Transforming how healthcare information is managed in the cloud

As large volumes of healthcare data continue to grow, many healthcare organizations are turning to the cloud for secure content management, workflow, and collaboration, as well as to power mission-critical business processes. Key challenges faced by healthcare providers include secure on-site and mobile access to patient information for clinicians and doctors, interoperability between organizations to share patient medical records and an increasingly digital-first patient base demanding online and mobile-based provider-patient communication. As a cloud content management solution that supports HIPAA (Health Insurance Portability and Accountability Act) compliance, Box enables healthcare organizations to address these challenges. Our customers leverage Box across a variety of use cases, including coordinated patient care, streamlining the patient journey from appointment scheduling to follow-up, and secure patient portals. Fundamentally, we believe that quality care begins with privacy and security and have taken specific steps to ensure we support HIPAA compliance. This is provided for informational purposes only and should not be construed as legal advice. Customers should consult with their own legal, privacy and security teams to ensure that customers meet their obligations under HIPAA, including using and configuring the Box service and products in a HIPAA-compliant manner.

HIPAA compliance with Box

HIPAA is a U.S. federal mandate that requires protections for Protected Health Information (PHI). Box supports HIPAA compliance, including the final Omnibus rule and Health Information Technology for Economic and Clinical Health (HITECH) Act. Box provides to its eligible customers a Business Associate Agreement (BAA) which meets HIPAA requirements. There are no official government or industry certifications to validate if a technology solution is, in fact, 'HIPAA compliant'. Box has implemented security and privacy controls to enable customers to meet the requirements set forth by HIPAA. These controls are reviewed as part of our annual SOC 2 audit, and Box has been assessed and received the 'Avertium' and ISO 27001 certifications. Additionally, Box has passed numerous customer security and compliance audits for storing and handling PHI prior to deployment in hospital and health systems, universities, life sciences companies as well as in organizations in non-regulated industries subject to HIPAA. On top of this, customers will need to ensure they configure their Box environment in a HIPAA-compliant manner to meet their HIPAA obligations, including the retention of documentation about the policies and procedures put in place to meet HIPAA.

"For any healthcare organization, privacy, security and trust is paramount. MD Anderson is able to empower faculty, staff, researchers, and physicians around the world in the new ways they want to work. We are improving patient care, while still meeting critical compliance requirements by using Box"

Jeff Frey
Information Services Director
University of Texas
MD Anderson
Cancer Center

A **Covered Entity** stewards Protected Health Information (PHI) on patients in the process of providing care or paying for care. This includes healthcare providers, such as doctors and clinics, as well as health plans and healthcare clearinghouses.

A **Business Associate** refers to a person or organization that conducts business with a Covered Entity and touches the PHI held by the Covered Entity. Examples include vendors that provide software solutions. Box is a Business Associate and signs HIPAA Business Associate agreements with its customers.

Box has taken a careful and controlled approach to supporting HIPAA compliance for our customers by focusing on three key pillars:

- Product features, security, and infrastructure
- Legal requirements
- Box policies and procedures

Pillar I: Key product features, security, and infrastructure

Product features:

- **Content protection.** Box provides content integrity protection through versioning and deletion controls, but can also enforce content security policies or quarantine content that doesn't comply. For more advanced Data Loss Protection (DLP) rules, Box integrates with multiple DLP vendors and Cloud Access Security Brokers (CASBs) including Symantec, Skyhigh, CipherCloud, and Netskope.

Symantec. Skyhigh CipherCloud netskope

- **Audit trail and logging.** Box maintains an audit trail of activities for both users and content. A comprehensive set of logs show who accessed what content and the action taken on it (e.g., who modified the file, when it was previewed, commented on, downloaded, etc.).
- **Access control.** Box provides access controls to content with granular permissions. This allows customersto define user roles for access to content by offering 7 different access levels for folder collaborators and 10 options for shared links. Further, Box allows you to monitor, revoke, and expire access to content at any time.
- **Information governance.** Box Governance provides content lifecycle management to reduce risk without impacting productivity. It offers flexible retention and disposition schedules, preservation for defensible discovery, and trash controls. For instance, organizations can enforce retention policies on PHI to maintain and safeguard medical records for appropriate durations to meet their requirements to retain HIPAA-related documentation per CFR §164.316(b)(2)(i). Further, Box Governance provides controls for in-place preservation to place legal holds on content where required formal practice and other litigation claims.
- **Medical image viewer.** The Box DICOM Viewer is an FDA-cleared Class II Medical Device for diagnostic viewing. It allows users to store, view and share DICOM files (X-rays, CT scans, Ultrasounds and MRIs) securely in the cloud. This enables sharing of imaging studies across healthcare organizations with patients or with referring physicians, without needing to transfer information across multiple systems.
- **Automated workflows.** Box Relay simplifies and streamlines critical time-consuming tasks by enabling users to create self-service workflows completely within Box, without having to rely on external systems. For instance, patient referral workflows can seamlessly handle information flow between the referring physician and the specialist care provider. Further, Box also integrates with specialized workflow and business process management solutions, such as Nintex, Pega Systems, Workato, etc., as well as eSignature providers like DocuSign and AdobeSign for CFR Part 11 compliance. This significantly increases process efficiency and reduces paperwork.

nintex PEGA workato DocuSign Adobe Sign

Security:

- **Data encryption at rest and in transit.** 256-bit AES encryption at rest with support for TLS 1.1–1.2 in-transit.
- **Authentication & Identity Management.** Box offers multiple ways to authenticate authorized users, such as Active Directory and SSO integration, to provision and manage accounts easily by connecting with corporate identity services. Operating on SAML-based open standards, Box works withall major SSO providers, such as Okta, Ping, OneLogin, etc.

- **Alerts, reporting, and analytics.** All user activity in Box is logged for reporting and monitoring purposes. Additionally, Box supports integration with SIEM (Security Information and Event Management) partners, such as Splunk and SumoLogic, and BI (Business Intelligence) systems, such as Tableau and Domo. This enables visibility into actions of users inside theorganization, as well as external collaborators. With real-time reporting, organizations can achieve full transparency across every event, user, and administrative action.

- **External collaboration.** For sharing content with external parties, organizations can enforce the use of strong passwords, enforce two-factor authentication, as well as require acceptance of customer's 'custom terms of use' before allowing external users into collaborated folders.
- **Mobile device security.** Box natively offers device pinning and remote logout capabilities. It also integrates with Mobile Device Management (MDM) vendors like MobileIron and Airwatch for additional security and control for mobile devices.

- **Intelligent security.** Box Shield offers content classification guardrails to prevent user mistakes and compromise, and advanced threat detection of unusual behavior to protect againstmalicious actors. For example, classification-driven security policies can prevent accidental leakage of information with a designated classification, such as PHI.

Infrastructure:

- **Secure and reliable access to data.** Box uses data centers that undergo independent SSAE 18 Type II SOC 1 audits. We have two mirrored data center facilities set up in an active-active configuration to provide a 99.9% uptime SLA.
- **Disaster recovery.** Box has a disaster recovery (DR) data center in a geographically remote location to address disaster scenarios.

Pillar II: Key legal requirements

Box is a HIPAA Business Associate to its eligible customers with which it enters into BAAs and Box serves both Covered Entities and other Business Associates as partof its healthcare customer base. Box provides BAAs to its eligible customers.

Box applies the same, extensive security and privacy controls across the service platform, regardless of the customer account plan. However, customers who are required by law to comply with HIPAA must have an eligible Box account plan that is capable of being configured in a manner compliant with HIPAA in order to execute a HIPAA BAA with Box. HIPAA requires a BAA to be in place with most service providers who process PHI, so please contact Box to execute a BAA prior to storing any PHI in Box.

Pillar III: Key Box policies and procedures

Box security policies serve as another critical pillar of support for HIPAA compliance, further ensuring the privacy and security of your data.

- **Breach notification.** Box has a formally defined and tested breach detection and notification policy.
- **Employee training.** Box employees undergo regular training on security policies and controls.
- **Restricted access.** Employee access to customer data, as well as physical access to production servers is highly restricted.

While the Box product, service, and business practices provide a platform that can be configured to meet HIPAA requirements, customers who use Box to store PHI are responsible for configuring Box to meet HIPAA requirements, as well as their own organizational requirements. Many of our customers leverage Box add-ons like Box Governance, Box KeySafe, and Box Shield to configure and administer the Box service to enforce their internal policies related to HIPAA. Additionally, our Box Consulting service has deep expertise in providing best practices in configuring Box for healthcare companies and PHI use cases. Box was one of the first cloud-based applications to support HIPAA compliance, and has been actively supporting customers' PHI use cases for over 7 years.

To learn more, visit www.box.com/healthcare.