Dropbox and FDA 21 CFR Part 11

Dropbox Business

11.10 Controls for Closed Systems

Requirements

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.

Such procedures and controls shall include the following:

11.10 (a)

Requirements

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

How Dropbox Supports Compliance

Processing integrity is at the core of the Dropbox Business and Dropbox Education services. Dropbox has implemented several processes and controls to validate that each file and Paper doc maintains its integrity and is not corrupted during each step of the process: creation, upload, processing, storage, download, and deletion.

For more information, please see the System and Network Summary in the latest SOC 2 Type II attestation, which addresses the SOC 2 Trust Services Criteria for Processing Integrity and Availability.

11.10 (b)

Requirements

The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

How Dropbox Supports Compliance

Dropbox maintains internal controls, user processing controls, and security controls to ensure that users are able to inspect, review, and copy electronic records. Dropbox logs user and administrator log-on and file sharing activities for Dropbox Business users. Dropbox makes the logs available to administrators in industry standard read-only format.

For more information about admin permissions, please see this **Help Center Article** and the Monitoring and System Operations section in the latest SOC 2 Type II attestation.

11.10 (c)

Requirements

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

How Dropbox Supports Compliance

Dropbox file data and Paper docs are encrypted and stored on Dropbox Infrastructure and AWS, respectively. Dropbox file data is replicated across multiple data centers. Dropbox performs full backups of metadata and Paper doc data. The admin dashboard maintains a complete audit log of dates, times, and information about who accessed files and docs and from what location. Documents can be accessed by authorized users at any time during the retention period.

For more information, please see the Availability section of our latest SOC 2 Type II attestation and these Help Center Articles on Monitoring team sharing activity and recovering deleted files.

11.10 (d)

Requirements

Limiting system access to authorized individuals.

How Dropbox Supports Compliance

Dropbox maintains security controls that restrict any unauthorized distribution, access to, or use of electronically-stored records. Dropbox provides administrator controls over end-user account authentication, registration, and de-provisioning. These functionalities ensure that only authorized individuals are able to access Dropbox files, folders, and Paper docs.

Dropbox also maintains user communications and product controls to enable Dropbox admins and team users to protect against unauthorized access. Within the Dropbox admin dashboard, administrators can easily manage team member access to files, folders, and Paper docs. For shared file links, Dropbox's link permissions feature allows users to password protect the shared links, set expiration dates to grant temporary access, and limit access to those within the organization.

For more information about Dropbox's security controls and user communication, please see the Logical and Physical Security section and Communications section in the latest Dropbox SOC 2 Type II attestation.

11.10 (e)

Requirements

Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

How Dropbox Supports Compliance

Dropbox audit logs and activity reports can help support user record keeping. Activity report entries include date and time of the action, the member that initiated the action, details about the event itself, and the location and IP address of the user that initiated the action.

For more information, please see these Help Center Articles about monitoring file activity at Dropbox and viewing team activity in the admin console.

11.10 (f)

Requirements

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

How Dropbox Supports Compliance

Dropbox allows organizations to define business processes, including sequencing of steps and events, as appropriate for their electronic records. These steps can be enforced throughout user organizations to ensure consistency and compliance.

11.10 (g)

Requirements

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

How Dropbox Supports Compliance

Dropbox maintains security controls that restrict any unauthorized distribution, access to, or use of electronically-stored records. Dropbox service can be accessed only by individuals who own the account or authorized by the team administrator for an organization/business. Files or folders can only be accessed by users, and their Dropbox Business (Standard, Advanced, or Enterprise) or Dropbox Education administrator(s), who:

- Have the file or folder listed in their own Dropbox file directory
- Have received a link to the file or folder that has been initially shared by a user who had the file listed in their own Dropbox directory or by Dropbox Business (Advanced or Enterprise) team administrator(s) who:
  - Use the “Sign In as User” functionality provided to them in the Administrator Console

At this time, Dropbox and HelloSign do not offer compliance support under 21 CFR Part 11 specific to electronic signatures.

For more information about Dropbox security controls, please see the Logical and Physical Security section in the latest Dropbox SOC 2 Type II attestation.

11.10 (h)

Requirements

Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

How Dropbox Supports Compliance

Processing integrity is at the core of the Dropbox Business and Dropbox Education services. Dropbox has implemented several processes and controls to validate that each file and Paper doc maintains its integrity and is not corrupted during each step of the process: creation, upload, processing, storage, download, and deletion. This applies to desktop, web, or mobile clients.

For more information, please see the Processing Integrity section in the latest Dropbox SOC 2 Type II attestation.

11.10 (i)

Requirements

Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

How Dropbox Supports Compliance

Dropbox provides information and support to customers by maintaining blogs, a help center, forums, and through the Dropbox website and applications.

A description of the Dropbox Business and Dropbox Education systems and their boundaries is available to users via the Dropbox help center and the Dropbox Business Security Whitepaper on the Dropbox website. Details made available through the Dropbox website include features, usage guidelines, and additional information.

Dropbox's and our customers' security and confidentiality responsibilities are communicated via the Shared Responsibility Guide on the Dropbox website and through a combination of online documents, which include installation, setup, and configuration guidelines.

11.10 (j)

Requirements

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

How Dropbox Supports Compliance

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

Dropbox Business

11.10 (k)

Requirements

Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

How Dropbox Supports Compliance

(1) Dropbox maintains security controls that restrict any unauthorized distribution, access to, or use of electronically-stored records. This includes but is not limited to authentication requirements, access requirements, end-user account authentication, registration, and deprovisioning, file and data encryption, malware protection, and vulnerability patching.

For more information, please see the latest Logical and Physical Security section in the latest Dropbox SOC 2 Type II attestation.

(2) Dropbox maintains security controls and user processing tools that log user and administrator activity, including activity such as viewing Dropbox account information or actions taken on Dropbox accounts. For Dropbox Business and Dropbox Education plans, Dropbox logs user and and administrator log-on and file sharing activities, as well as account provisioning, de-provisioning, and any “sign in as user” activity. This allows users to maintain and track audit trails of any revisions or changes to system documentations.

For more information about monitoring file activity in Dropbox, please see this **Help Center article**.

Dropbox Business

11.10 Controls for Open Systems

Requirements

The company shall employ procedures and controls designed to ensure the authenticity, integrity, and confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate and additional measures such as document encryption.

How Dropbox Supports Compliance

In addition to the controls outlined in Section 11.10, Dropbox implements controls to validate and ensure the integrity of Dropbox files and Paper docs.

For more information, please see the Processing Integrity section in the latest Dropbox SOC 2 Type II attestation.

Disclaimer

We're pleased to provide information to help support our customers' compliance with FDA 21 CFR Part 11. However, the information above is not intended to be legal advice. We recommend you consult an attorney if you have any legal questions.