Transmitting Electronic Records with Aspera

A Review of how the Aspera platform Meets 21 CFR Part 11 Compliance Criteria

February 2018

WHITE PAPER

aspera
an IBM® company

Transmitting Electronic Records with Aspera

aspera
an IBM® company

This whitepaper details how the Aspera platform provides secure authentication, data integrity verification, access control and detailed tracking and reporting tools that organizations need to meet the criteria set forth in 21 Code of Federal Regulations (CFR) Part 11.

INTRODUCTION

In the early 1990s, key groups within the pharmaceutical industry met with the Food and Drug Administration (FDA) to determine how companies in FDA-governed industries must handle electronic records and signatures as an extension of the guidelines set forth under the authority of the FDA by the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act. The regulation is grounded in the agency's belief that new data technologies have become pervasive and established 21 CFR Part 11 to minimize the possibility of data misappropriation.

The criteria, effective since August 20, 1997, considers electronic records to carry the same compliance requirements as paper records, and electronic signatures as an equivalent to the traditional wet ink handwritten signatures. From the year 2000, the FDA has released a number of guidance papers in response to the changing landscape in an effort to clarify the rule and how it should be interpreted.

21 CFR Part 11 applies to electronic records and signatures that are created, modified, maintained, archived, retrieved or transmitted by FDA regulated industries such as drug makers, medical device manufacturers, biotech companies, biologics developers, and contract research organizations.

While the use of electronic records and signatures are not mandated, 21 CFR Part 11 establishes a standard criteria by which it is considered trustworthy and reliable. 21 CFR Part 11 requires regulated companies to implement and document controls including audits, system validations and audit trails for software and systems that utilize electronic records and signatures as the authoritative document in place of "hard copy."

This whitepaper provides the information to help you be in compliance with Part 11 requirements when transmitting electronic records with any Aspera product offering, all of which are built on a single platform, herein referred to as the Aspera Platform.

ASPERA PLATFORM 21 CFR PART 11 STATEMENT

Section	Description	Summary	Features
11.10	**Controls for closed systems**		
11.10(a)	Validation of systems to ensure accuracy, reliability and intended consistent performance, and the ability to discern invalid or altered records.	System Validation	The Aspera Platform is validated by IBM Aspera to ensure accurate, reliable and intended performance of the Aspera system. Installation Qualification/Operational Qualification (IQ/OQ) procedures for the proper function of the Aspera Platform can be put into place. Data uploaded to the Aspera Platform cannot be altered in situ, only downloaded or deleted.
11.10(b)	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.	Record generation and copying	The Aspera Platform stores electronic records only. APIs exist to create a human-readable list of all records on the platform.

Transmitting Electronic Records with Aspera

aspera
an IBM® company

Section	Description	Summary	Features
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Record protection	The Aspera Platform can be configured to encrypt files or folders at rest, which prevents modification of the data stored on the platform. User records are available only when a person authenticates themselves using their email and password or to administrators who also need to authenticate using their email and password.
11.10(d)	Limiting system access to authorized individuals.	Access limitation	The Aspera Platform requires all users to login using their email and password for platform access. Each user has a defined role, including access privileges.
11.10(e)	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.	Audit Trails	Time-stamped audit trails are recorded for all file storage and transfer activities.The audit trails are stored in text format and entries cannot be overwritten.
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Operational system checks	Not applicable.
11.10(g)	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.	Authority checks	The Aspera Platform ensures that users have proper permissions to carry out defined functions based on their role and access privileges. It is the responsibility of the operating company to ensure that each username can be traced to a real individual and to ensure appropriate privileges.
11.10(h)	Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Device/terminal checks	The Aspera Platform applies checks to allow only valid information input in respective fields.
11.10(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Training and user accountability	IBM Aspera ensures developers are fully and continuously trained; and provides IBM Aspera Software user training. The operating company is responsible for training on their standard operating procedures (SOP) in regards to electronic records and electronic signatures.

Transmitting Electronic Records with Aspera

aspera
an IBM® company

Section	Description	Summary	Features
11.10(j)	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.		Not applicable.
11.10(k)	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.	System Document Control	A release-specific software manual is distributed together with the IBM Aspera Software. IBM Aspera Software development is governed by a design and change control process that ensures the creation and tracking of relevant documents.
11.30	**Controls for open systems**		**Responsibility of the operating company.**
11.50	**Signature manifestations**		**Not applicable. The Aspera Platform does not create electronic signatures.**
11.70	**Signature/record linking**		**Not applicable. The Aspera Platform does not create electronic signatures.**
11.100	**Electronic signatures**		**Not applicable. The Aspera Platform does not create electronic signatures.**
11.200	**Electronic signature components and controls**		**Not applicable. The Aspera Platform does not create electronic signatures.**
11.300	**Controls for identification codes/ passwords**		
11.300(a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Uniqueness of ID/ password	The Aspera Platform user management system ensures that all user IDs are unique. If the software is configured to use a directory service (i.e. SAML), it is the responsibility of the operating company to ensure that user ID and password used within the SAML system are unique.

Transmitting Electronic Records with Aspera

aspera
an IBM® company

Section	Description	Summary	Features
11.300(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Password aging	The Aspera Platform provides password expiration and account lockout after several authentication failures. Specific criteria should be set by the operating company. If the software is configured to use a customer's SAML system for user authentication, it is the responsibility of the operating company to ensure features such as password aging etc.
11.300(c)	Following loss management procedures to electronically deauthorize lost, stolen, missing or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Lost ID/password management	The Aspera Platform enables the administrator to manage user profiles, including user IDs and passwords. The Aspera user management as well as SAML configuration supports deauthorization. Proper loss management procedures are the responsibility of the operating company.
11.300(d)	Use of transaction safeguards to prevent unauthorized use of password and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Controls to prevent unauthorized credential use	The Aspera Platform will log the active user out after an inactive period of time to prevent unauthorized attempted use. Other transaction safeguards, such as supervision of blocked accounts, lies within the responsibility of the operating company.
11.300(e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	Periodic testing of ID/password generation	Not applicable. This is the responsibility of the operating company.

REFERENCES

Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application, August 2003
https://www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm125125.pdf

Guidance for Industry Computerized Systems Used in Clinical Investigations, May 2007
https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM070266.pdf