21 CFR Part 11 Compliance with TIBCO Data Science

Executive Summary

TIBCO is committed to partnering with our customers in meeting our mutual goal of design and production of products of the highest quality and reliability. Many of our customers in FDA-regulated industries, such as the design and manufacturing of pharmaceutical, food, and medical device products, rely on TIBCO Data Science software is an integral tool for their research, development, and quality control processes for meeting FDA 21 CFR Part 11 regulations.

Compliance with 21 CFR Part 11 entails both procedural and software requirements, and TIBCO Data Science software helps meet all of them: "Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations."

Using TIBCO Data Science

TIBCO Data Science software is used where 21 CFR Part 11 is relevant, including to:

- Test the characteristics of new products
- Optimize product formulations
- Inspect raw materials to be used in the manufacturing of products
- Judge the efficacy of multiple product configurations

- Predict product reliability
- Determine the most important process parameters within a multivariate product manufacturing application
- Certify that particular lots of product conform to specifications
- Produce annual product review reports
- Manually enter data

For each of these use cases, TIBCO Data Science software can be used to:

- Create data cleaning and data mashup templates
- Create analytic workflow templates
- Use templates
- Validate data
- Write validated data back into a database
- Email tabular and graphical results
- Generate summary reports as PDFs
- Use dashboards

Depending on the use case, the data and results used may be subject to the rules of the 21 CFR Part 11.

TIBCO Data Science Compliance Solution

TIBCO Data Science Enterprise Manager

The TIBCO Data Science Enterprise Manager application is used to manage the metadata store objects (data access, analysis, templates, report configurations, analytic templates). This application uses role-based security, versioning, approving via electronic signature, and audit logs to control, monitor, and report. The application integrates with Active Directory.

TIBCO Data Science Data Entry Server

The TIBCO Data Science Data Entry Server integrates with TIBCO Data Science Enterprise Manager. Configuration of web forms, which are used for manual data entry, is managed with TIBCO Data Science Enterprise Manager. When an employee manually enters data via https://[your-server-name]/dataentry, the web form will capture signatures, comments, and approvals.

This creates a system that satisfies 21 CFR Part 11 requirements. In addition, TIBCO Data Science software provides validation packages to assist in 21 CFR Part 11 validation.

Compliance Details

This section provides details on how TIBCO Data Science software complies with the relevant sections of 21 CFR Part 11. Excerpts from the regulation are provided in the left column.

SECTION	LIVE QUERIES/ IN-DATABASE	TIBCO DATA SCIENCE FEATURES
11.10	Controls for closed systems	
11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Read-only audit trail tracks login/ logout, creation, modification, deletion, approval of objects along with computer generated date/time stamp. Web forms can be configured to prevent invalid data from being saved with the "complete" status. To validate entered data, the user can select from a pull data list or only enter a number > .081 AND < .089. Very complex formulas can be written to use multiple fields from the web form. The web forms for manual data entry can use double blind data entry for verification of accuracy. Two individuals enter the same data (record). They mark the records as "complete." The system captures electronic signatures that the records are complete and compares the two records. If the records don't match, they are both rejected and email notification(s) are sent to correct the issue. If the two records are identical, the system marks one record as "approved."
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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of electronic records.	Audit logs can be retrieved, filtered, and saved as PDFs for easy sharing. Analytic results, metadata, or raw data can be viewed within the TIBCO Data Science system in spreadsheets or reports. This information can also be exported to Excel, Word, or sent by email. Manually entered data can be reviewed within a web browser or retrieved for analysis.
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	All records and their metadata, including older versions, can be readily retrieved, viewed, and used in reports.

SECTION	LIVE QUERIES/ IN-DATABASE	TIBCO DATA SCIENCE FEATURES
11.10(d)	Limiting system access to authorized individuals.	The TIBCO Data Science system integrates with Active Directory user accounts. When the TIBCO Data Science system is configured, we recommend setting up synchronization with the domain. This allows it to add and delete users based on domain groups. As long as the domain groups are kept updated, IT does not need to log in to the TIBCO Data Science system to add or delete users and existing security processes can be used. The system has multiple levels of security. The user has to be granted access to use a specific application. Within the application they need to be granted read or edit permissions to use specific configuration objects.
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.	The audit log options are configured shortly after installation. Actions such as login/logoff, create, modify, or delete can be logged with a change reason, date and time stamp, and user name. There is a configuration option to turn on audit logging and prohibit any changes to the logging. In other words, once this option is turned on, it cannot be turned off. Note: The delete action mentioned above is the deletion of a template or configuration object by an administrator. It is not possible to delete any manually entered data. It is not possible for a user to delete the audit log within the application.
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Users create analytic workflow templates to sequence data cleaning and analytic steps. They create validation rules and sequences for web forms used for manual data entry, such as: If “field 1 on form 1” > .066 then “field 2 on form 3” must be < .1, otherwise error and don’t let form 3 be saved. The sequence of create → edit → review → approve is handled within TIBCO Data Science Enterprise Manager.

SECTION	LIVE QUERIES/ IN-DATABASE	TIBCO DATA SCIENCE FEATURES
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.	The TIBCO Data Science system integrates with Active Directory login accounts, which use a combination of a username and password to authorize an electronic signature. The TIBCO Data Science system uses roles-based security and verifies if an individual has the right to start TIBCO Data Science software, manually enter data, review and approve manually entered data, create templates, use templates, modify a specific template, log in to a website, and other operations.
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.	The system uses role-based security to grant access to applications or objects within applications. Users are typically granted a role by belonging to a specific Active Directory group. The system collects electronic signatures (login and password that verify identity) when objects are approved or when manually entered data is marked "complete" and ready to validate.
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.	Responsibility of customer.
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.	Responsibility of customer.
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.	TIBCO Data Science user guides and admin guides are installed with the product. Release notes are available from the Support Portal. Documentation is identifiable as applying to its specific version.
11.30	Controls for open systems.	Not applicable
11.50	Signature manifestations.	

SECTION	LIVE QUERIES/ IN-DATABASE	TIBCO DATA SCIENCE FEATURES
11.50(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	When integrated login with Active Directory is used, then the electronic signature is the domain\login name and password that was used when signing into the computer. The system automatically captures the date and time stamp with the signature. The system can be configured to record the meaning of the signature.
11.50(b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	This information is displayed in a read-only audit trail. A report (PDF) can be generated with this information.
11.70	Signature/record linking. Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	An electronic signature is linked to a specific version of an object that contains information about the purpose of the signature and the record(s) it is intended to authorize. This linked information is stored in the metadata store. From within the system it is impossible to remove, modify, or transfer an existing electronic signature.
11.100	General Requirements.	
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	We recommend using integrated login with Active Directory. This requirement therefore will be enforced with AD and the customer's standard security processes.
11.100(b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Responsibility of customer.

SECTION	LIVE QUERIES/ IN-DATABASE	TIBCO DATA SCIENCE FEATURES
11.100(c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Responsibility of customer.
11.200	Electronic signature components and controls.	
11.200(a)	Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	We recommend using integrated login with Active Directory. This requirement therefore will be enforced with AD and the customer's standard security processes. The TIBCO Data Science system always collects the domain\login account and password for electronic signatures.

SECTION	LIVE QUERIES/ IN-DATABASE	TIBCO DATA SCIENCE FEATURES
11.200(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Not applicable. TIBCO Data Science software does not use biometric authentication techniques.
11.300	Controls for identification codes/passwords.	
11.300(a)	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Recommend integrating TIBCO Data Science software with Active Directory logins so the customer's established security processes can be used.
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).	Recommend integrating TIBCO Data Science software with Active Directory logins so the customer's established security processes can be used.
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.	Recommend integrating the TIBCO Data Science system with Active Directory logins so the customer's established security processes can be used.
11.300(d)	Use of transaction safeguards to prevent unauthorized use of passwords 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.	Recommend integrating the TIBCO Data Science system with Active Directory logins so the customer's established security processes can be used.

SECTION	LIVE QUERIES/ IN-DATABASE	TIBCO DATA SCIENCE FEATURES
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.	Recommend integrating the TIBCO Data Science system with Active Directory logins so the customer's established security processes can be used.

Summary

TIBCO Data Science software provides integrated solutions for compliance to 21 CFR Part 11 requirements. For more information about the details for your application, please contact us via https://www.tibco.com/contact-us.

Global Headquarters
3307 Hillview Avenue
Palo Alto, CA 94304
+1 650-846-1000 TEL
+1 800-420-8450
+1 650-846-1005 FAX
www.tibco.com

TIBCO fuels digital business by enabling better decisions and faster, smarter actions through the TIBCO Connected Intelligence Cloud. From APIs and systems to devices and people, we interconnect everything, capture data in real time wherever it is, and augment the intelligence of your business through analytical insights. Thousands of customers around the globe rely on us to build compelling experiences, energize operations, and propel innovation. Learn how TIBCO makes digital smarter at www.tibco.com.

29Oct2019