



StatSoft®

Business White Paper

21 CFR Part 11 Compliance Using *STATISTICA*

Last Updated: April 2003

This document was updated to reflect the FDA's latest guidance (released February, 2003) and the withdrawal of previous guidance.

U.S. Headquarters: StatSoft, Inc. • 2300 E. 14th St. • Tulsa, OK 74104 • USA • (918) 749-1119 • Fax: (918) 749-2217 • info@statsoft.com • www.statsoft.com

Australia: StatSoft Pacific Pty Ltd.
Brazil: StatSoft Brazil Ltda.
Czech Republic: StatSoft Czech Rep. s.r.o.
France: StatSoft France

Germany: StatSoft GmbH
Hungary: StatSoft Hungary Ltd.
Israel: StatSoft Israel Ltd.
Italy: StatSoft Italia srl

Japan: StatSoft Japan Inc.
Korea: StatSoft Korea
Netherlands: StatSoft Benelux BV
Poland: StatSoft Polska Sp. z o. o.

Portugal: StatSoft Iberica Ltda.
Russia: StatSoft Russia
Singapore: StatSoft Singapore
S. Africa: StatSoft S. Africa (Pty) Ltd.

Spain: StatSoft Espana
Sweden: StatSoft Scandinavia AB
Taiwan: StatSoft Taiwan
UK: StatSoft Ltd.

Table of Contents

Executive Summary	3
Overview of the Regulation	3
Relevance to <i>STATISTICA</i> Applications.....	4
<i>STATISTICA</i> 's Approaches for Compliance.....	4
The <i>STATISTICA Document Management System</i>	5
Conclusions	8
References	9

Executive Summary

StatSoft, provider of the **STATISTICA** product suite, is committed to partnering with our customers in meeting our mutual goal of the 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 and medical device products, rely on **STATISTICA** as an integral software tool within their Research and Development and Quality Control processes.

STATISTICA is used within organizations in applications where the FDA's 21 CFR Part 11 regulation is applicable. The **STATISTICA** software suite aids organizations in their compliance efforts by meeting all of the requirements of 21 CFR Part 11. StatSoft, through its Technical Services group, provides software validation services as part of the deployment of **STATISTICA** applications.

Overview of the Regulation

In 1997, the FDA released the final version of the 21 CFR Part 11 regulations. The regulation provides the framework in which organizations are able to produce, store and provide secure access to electronic records. The scope of the regulation includes any area where paper-based records had been required. 21 CFR Part 11 is relevant when those paper-based procedures, signatures, and storage techniques are to be replaced with electronic recordkeeping via a computer-based system. The regulation includes rules regarding the copying, audit trails, version control, access control, and signatures of electronic documents being stored and produced for compliance purposes.

As of the writing of this document, the FDA guideline is that 21 CFR Part 11 is not relevant where physical records are kept, including print-outs of computer-generated reports and documents that are then signed and archived.

Compliance with 21 CFR Part 11 entails both procedural requirements and software requirements. The procedural requirements include validating the electronic records system, drafting and maintaining standard operating procedures for the use of the electronic records system, and ensuring that users of the electronic records system have adequate training about its appropriate use and administration.

Relevance to *STATISTICA* Applications

STATISTICA is used for many applications where 21 CFR Part 11 is relevant. For example, *STATISTICA* is used by organizations:

- To test the characteristics of new products,
- To optimize product formulations,
- To inspect raw materials to be used in the manufacturing of products,
- To make judgments about the efficacy of multiple product configurations,
- To make predictions about product reliability,
- To determine the most important process parameters within a multivariate product manufacturing application,
- To determine the optimal product packaging for shipment, storage and delivery to consumers, and
- To certify that particular lots of product conform to product specifications.

For each of these applications, *STATISTICA* may be used for any combination of the following activities:

- To store data,
- To perform data management and cleaning tasks,
- To produce tabular and graphical output, and
- To produce summary reports of those analytic results.

Depending upon the application, the data and results used for these purposes may be subject to the rules of the 21 CFR Part 11 regulation.

STATISTICA's Approaches for Compliance

STATISTICA is compliant with the software requirements of 21 CFR Part 11 through at least two approaches:

1. ***STATISTICA Document Management System***: *STATISTICA* provides an integrated document management system for the storage, approval and archiving of data, results, reports, SOPs and any other document related to the *STATISTICA* application. The ***STATISTICA Document Management System*** satisfies all of the 21 CFR Part 11 requirements.

2. **Third Party Document Management Systems:** Where an organization already has a document management system, **STATISTICA** integrates with that system to communicate to its repository for the storage and retrieval of documents.

In addition, StatSoft Technical Services provides validation packages to assist our clients in the validation requirements of 21 CFR Part 11.

The *STATISTICA* Document Management System

This section provides details of how the **STATISTICA Document Management System** complies with the relevant sections of 21 CFR Part 11. Excerpts from the regulation are provided in bold text.

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

StatSoft provides validation services as part of its installation and qualification of the **STATISTICA**-based application.

§ 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.

Records include **STATISTICA** Documents such as Spreadsheets and Graphs, as well as image files, MS Word or Excel documents, PDF, text files, etc. **STATISTICA** documents stored in the system can be accessed and viewed/printed from within the **STATISTICA** environment. Using the client application, all document types can be copied to the local machine and viewed/printed in their native applications.

§ 11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

All records and their metadata, to include historical versions, can be readily retrieved. The **STATISTICA Document Management System** stores all versions of all files without automatically deleting or removing previous versions.

§ 11.10(d) Limiting system access to authorized individuals.

The system has multiple levels of security. Each user is assigned an account with a unique username and password, both of which are required to log on to the system.

The user's identity and role are combined with the access control system attributes of one or more documents to determine whether access to a procedure on a document should be permitted or denied.

§ 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.

Each action performed in the system including modifying, creating, and deleting documents are written automatically to audit trail tables in the system's database.

§ 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 **STATISTICA Document Management System** uses a combination of a username and password to authorize an electronic signature.

§ 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.

The **STATISTICA Document Management System** documentation is updated and distributed with each version of the software. Each set of documentation, including, User manuals and Administrator manuals, are uniquely identifiable as applying to its specific version.

§ 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.**

An electronic signature is executed by the user through the user interface of the application, whereupon the user is required to enter her username and password (see

11.200.) The electronic signature is stored in the database along with the name of the unique identifier of the document, the signer's full name, the date and time the signature was executed, and the meaning of the signature. When viewing or printing the record from within the system, a signature page is displayed / printed which will include all required items.

§ 11.70 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 stored within the system in a relational database that maintains a link between the record and the signature. From within the system it is impossible to remove, modify, or transfer an existing electronic signature. An electronic signature is linked to a specific version of a specific document.

A handwritten signature applied to a paper document which is then transferred to an electronic format and placed in the system is under the same controls as any other document in the system including tracking of modifications and audit trail, and therefore the signature cannot be excised, copied, or transferred using ordinary means.

§ 11.100(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

Each username/password combination is unique. User accounts can be disabled by an administrator but cannot be removed from the system, thus the system enforces that the signature cannot be reused or reassigned.

§ 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.

§ 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.

The **STATISTICA Document Management System** does not use biometric authentication techniques. Instead, a user of the system enters her username and password combination to authorize a signature.

§ 11.300 Controls for identification codes/passwords. 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:

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.

The **STATISTICA Document Management System** enforces the requirement that the each combination user id / password is unique.

§ 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).

The **STATISTICA Document Management System** allows for passwords to expire after a set period of time.

Conclusions

STATISTICA provides integrated solutions for compliance to 21 CFR Part 11 requirements. For more information about the details of an approach for your application, contact StatSoft Technical Services at 918-749-1119 and make reference to this document.

References

1. 21 CFR Part 11. Electronic Records; Electronic Signatures; Final Rule Electronic Submissions; Establishment of Public Docket; Notice. March 20, 1997.
2. Draft Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application. February, 2003.