


# TopSpin GxP

- 21 CFR Part 11 Compliance Document

Version 002



Copyright © by Bruker Corporation

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means without the prior consent of the publisher. Product names used are trademarks or registered trademarks of their respective holders.

© October 07, 2021 Bruker Corporation

Document Number:

P/N: H181366

---

# Contents

<b>1</b>	<b>21 CFR Part 11 Compliance Document .....</b>	<b>5</b>
1.1	Subpart B - Electronic Records.....	7
1.1.1	Sec. 11.10 Controls for closed systems.....	7
1.1.2	Sec. 11.10(a) .....	7
1.1.3	Sec. 11.10(b) .....	7
1.1.4	Sec. 11.10(c).....	8
1.1.5	Sec. 11.10(d) .....	9
1.1.6	Sec. 11.10(e) .....	11
1.1.7	Sec. 11.10(f) .....	14
1.1.8	Sec. 11.10(g) .....	14
1.1.9	Sec. 11.10(h) .....	16
1.1.10	Sec. 11.10(i).....	16
1.1.11	Sec. 11.10(j).....	17
1.1.12	Sec. 11.10(k).....	17
1.1.13	Sec. 11.10(k) (1) .....	17
1.1.14	Sec 11.10(k) (2) .....	18
1.1.15	Sec. 11.30 Controls for open systems .....	20
1.1.16	Sec. 11.50(a) Signature manifestations .....	20
1.1.17	Sec. 11.50(b) Signature manifestations .....	20
1.1.18	Sec. 11.70 Signature / record linking .....	21
1.2	Subpart C - Electronic Signatures.....	22
1.2.1	Sec. 11.100 General requirements .....	22
1.2.2	Sec. 11.100(a) .....	22
1.2.3	Sec. 11.100(b) .....	22
1.2.4	Sec. 11.100(c).....	23
1.2.5	Sec. 11.100(c) (1) .....	23
1.2.6	Sec 11.100(c) (2) .....	23
1.2.7	Sec. 11.200 Electronic signature components and controls .....	24
1.2.8	Sec. 11.200 (a) .....	24
1.2.9	Sec. 11.200(a) (1) .....	24
1.2.10	Sec. 11.200(a) (1i) .....	24
1.2.11	Sec. 11.200(a) (1ii) .....	24
1.2.12	Sec. 11.200(a) (2) .....	25
1.2.13	Sec. 11.200(a) (3) .....	25
1.2.14	Sec. 11.200(b) .....	25
1.2.15	Sec. 11.300 Controls for identification codes/passwords .....	25
1.2.16	Sec. 11.300(a) .....	25
1.2.17	Sec. 11.300(b) .....	26
1.2.18	Sec. 11.300(c).....	26
1.2.19	Sec. 11.300(d) .....	26
1.2.20	Sec. 11.300(e) .....	27
<b>2</b>	<b>Appendix A.....</b>	<b>29</b>

3    **Appendix B**..... 33

**Revision History** ..... 37

4    **Contact** ..... 39

**List of Figures**..... 41

# 1 21 CFR Part 11 Compliance Document

The text and citations of **21 CFR 11** have been worked out with the utmost care. However, we cannot accept either legal responsibility or any liability for any incorrect statements which may remain, and their consequences. The following publication is protected by copyright. All rights reserved. No part of this publication may be reproduced in any form by photocopy, microfilm or other procedures or transmitted in a usable language for machines, in particular data processing systems without our written authorization. The rights of reproduction through lectures, radio and television are also reserved. Some software referred to in this manual has a registered trademark and as such is subject to legal requirements.



This document is part of the TopSpin™ NMR software and is subject to changes without notice.

This document applies to TopSpin 4.1.0 GxP and higher versions.

## General

TopSpin is a software package for the control of Bruker BioSpin NMR Spectrometers, for data manipulation, analysis and presentation. It can be used in direct connection with the spectrometer or as a standalone "data station" version. Spectrometers running TopSpin as their spectrometer software may be used in companies/institutions that are legally bound to quality regulations. One of these regulations is the US regulation "**21 CFR Part 11 – Electronic Records; Electronic Signatures**" (details see below).

**21 CFR Part 11** is a document issued by the United States Food and Drug Administration (FDA). The title of this document is "**21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule**" (Source: 62 FR 13464, Mar. 20, 1997, unless otherwise noted) and it deals with electronic records and electronic signatures as a replacement for printed documents and hand-written signatures.

**21 CFR Part 11** was introduced by the FDA in 1997. For Scope – see [Appendix A \[ 29\]](#).

More detailed information about **21 CFR Part 11** can be found via Internet on <https://www.ecfr.gov/cgi-bin/text-idx?SID=9a86a3d23db4b1fd744009e49198be71&mc=true&node=pt21.1.11&rgn=div5>.

The current status and interpretation of these regulations has been put together by the GAMP Special Interest Group Forum and is available as a final draft "**Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures**" (dated September 2000) and in February 2005 an additional Good Practice Guide „*A Risk-Based Approach to Compliant Electronic Records and Signatures*“ was also published by the GAMP Special Interest Group.

See also FDA "**Guidance for Industry Part 11, Electronic Records; Electronic Signatures – Scope and Application**" from August 2003, Pharmaceutical CGMPs or latest revision.



*Requirements of EudraLex – Volume 4 – Good Manufacturing Practice (GMP) guidelines: Annex 11 – Computerized Systems (revision January 2011)* are also taken into consideration.

## Purpose

The purpose of this document is to give a comprehensive overview how the regulations within **"21 CFR Part 11"** are supported by TopSpin in order to assist companies in the validation of their systems.

## **PART 11 ELECTRONIC RECORDS; ELECTRONIC SIGNATURES**

**21 CFR part 11** is divided into three subparts:

- **Subpart A:** General Provisions
- **Subpart B:** Electronic Records
- **Subpart C:** Electronic Signatures

**Subpart A** comprises scope, implementation and definitions of the regulation and therefore does not lie within the scope of this document.

For completeness and for your information subpart A is reprinted in Appendix A.

All regulations of **Subpart B and C** including those sections not applicable to system vendors are covered by this document and put together in chapter form.

The chapters show for each of the sections how the regulations of **21 CFR Part 11** are supported by features designed into the TopSpin software.

The compliance chapters are organized as follows:

## Chapter Title:

**Section of 21 CFR Part 11**

## Chapter Content:

## Extract of 21 CFR Part 11:

Text of all **"21 CFR Part 11"** sections of **Subpart B and C**.

## Responsibility:

Shows the status of compliance/support by TopSpin.

There are five different categories:

- **Complies:** TopSpin fully complies with the regulations
- **Support:** TopSpin features facilitate compliance with the regulations
- **System owner:** This regulation is solely the responsibility of the system owner
- **Bruker support:** Bruker can give additional support for regulations for which the system owner is responsible
- **Does not apply:** The regulation does not apply to TopSpin

## BBIO Answer:

Describes how the regulations are handled or supported by TopSpin *GxP Regulatory Compliance User Manual*.

Additional information how the task has been implemented or carried out by Bruker BioSpin.

Where applicable, screenshots of the action seen by the user on the system monitor, are shown in the respective chapters.

Some of the screenshots shown here may look different to those on screen depending on the TopSpin version being used. However, the general functionality has remained unchanged up to the date of publication of this document and the TopSpin versions that has been included within it.

## 1.1 Subpart B - Electronic Records

---

Subpart B – Electronic Records<sup>1</sup>

### 1.1.1 Sec. 11.10 Controls for closed systems

---

#### **Extracted Text of 21 CFR Part 11**

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 sub-sections a-k.

**Responsibility:** System Owner

#### **BBIO Answer**

It is assumed that TopSpin is run as a closed system.

If TopSpin shall be run in an open system, the system owner has to establish suitable measures to prevent unauthorized access to the whole system or part of it.

### 1.1.2 Sec. 11.10(a)

---

#### **Extracted Text of 21 CFR Part 11**

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

**Responsibility:** Complies

#### **BBIO Answer**

TopSpin is validated based on a validation SOP. Bruker Document Product Validation Form: TOPSPIN Test Procedures. See latest approved version which is available on request after signing a non-disclosure agreement (NDA) with Bruker prior to audit.

All departments (on-site) of Bruker BioSpin are ISO 9001 compliant. See Scope of Bruker multisite certificate on the Bruker Homepage under: <https://www.bruker.com/en/about/quality.html>

Additional information about complete spectrometer system validation is available in the document Good Laboratory Practice (GLP) Requirements (Bruker Document Part Number # Z31619) on the Bruker Homepage under: <https://www.bruker.com/protected/en/services/user-manuals/nmr/glp.html>

Please note: A login is required.

### 1.1.3 Sec. 11.10(b)

---

#### **Extracted Text of 21 CFR Part 11**

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.

**Responsibility:** Complies

#### **BBIO Answer**

---

<sup>1</sup> Revised as of April 1, 2016

TopSpin data sets can be exported in JCAMP-DX format (which is an internationally standardized ASCII coded data exchange format). TopSpin JCAMP-DX files are as secure as TopSpin binary files and include the audit trails and any electronic signatures if they have been applied, together with a checksum covering the complete JCAMP-DX file.

Select **File | Save as**. Save the data set in a JCAMP-DX-file and click **OK**.

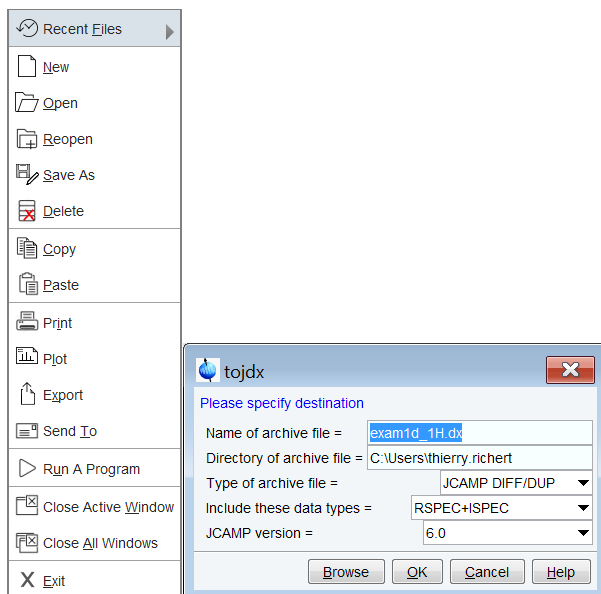


Figure 1.1: JCAMPDX

### 1.1.4 Sec. 11.10(c)

#### Extracted Text of 21 CFR Part 11

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

**Responsibility:** System Owner

#### BBIO Answer

This aspect is the responsibility of the system owner, TopSpin provides support, for example in the form of the **lockdataset** command:

Select **Manage | Security | Lock Data Set Against Changes (lockdataset)** The command **lockdataset** can also be used as part of AU scripts such as the one defined in the processing AU program (AUNMP).



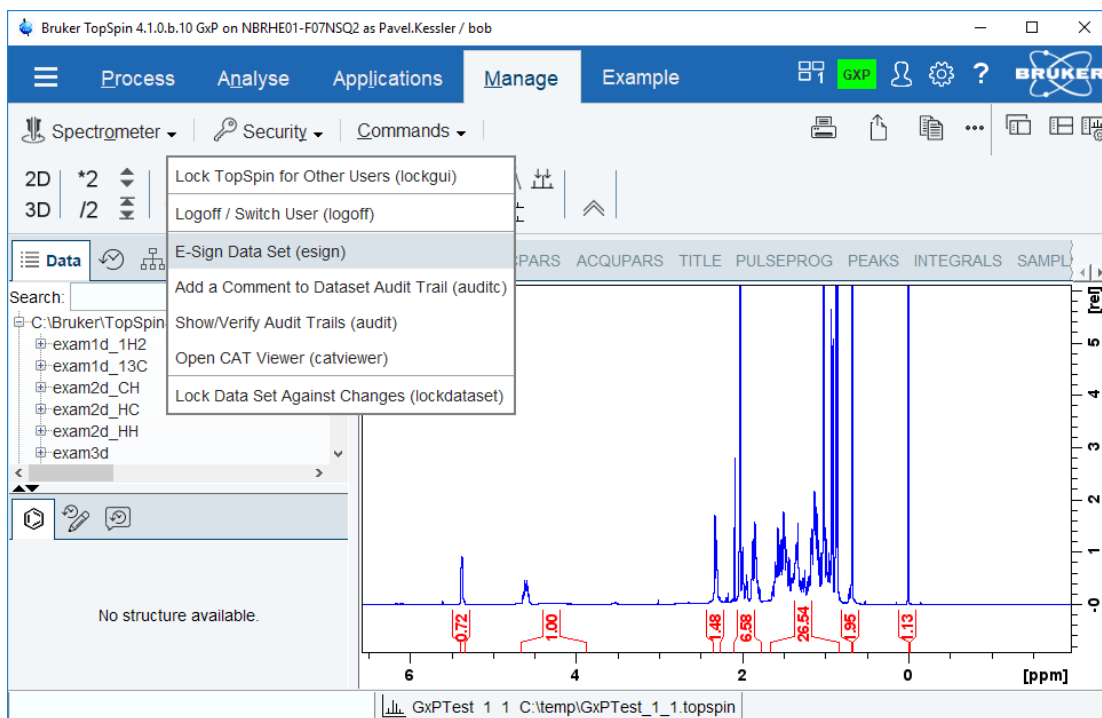


Figure 1.2: Lock Data Set Against Changes

### 1.1.5 Sec. 11.10(d)

#### Extracted Text of 21 CFR Part 11

Limiting system access to authorized individuals.

**Responsibility:** Complies

#### BBIO Answer

System access can be controlled by a two-level security system.


Level one is offered by the user management and security features of the operating system (OS) itself (Windows or Linux). TopSpin respects the file permission settings defined by the administrator at OS level. Follow the instructions given by your operation system (e.g. with Microsoft see the sample screen shot below).



Figure 1.3: Microsoft Operating System Account.

The second level of system access controls provided by TopSpin are shown below.

Topspin GxP includes a user identity management component which is independent on the

operating system. The desktop icon  opens the Identity Management (IM) console "Keycloak" where the Topspin users may be defined.

The IM console requires authentication – the Keycloak administrator name and password, which were set during the Topspin GxP installation.

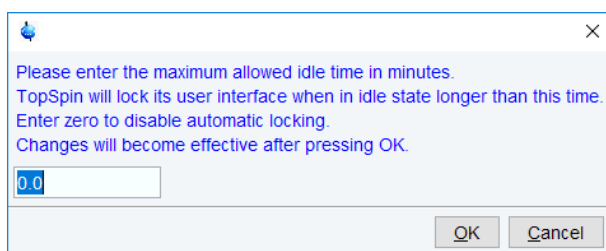
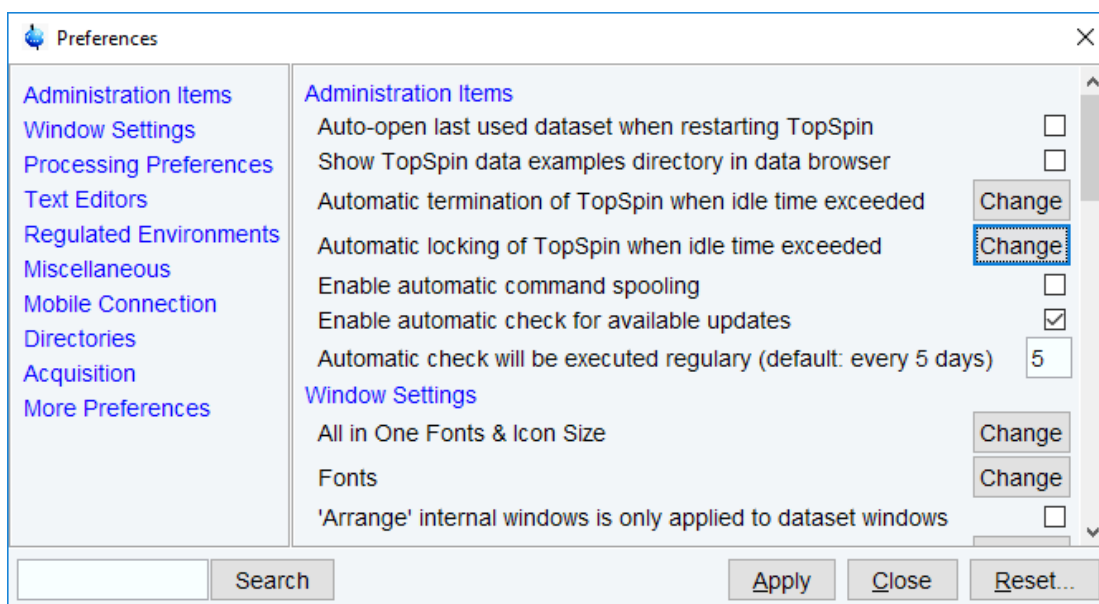
Topspin GxP always requires user authentication.

Each user defined in the IM has assigned a role, defining the allowed user activities like data processing, or spectrometer administration. Users without an assigned role are not allowed to log in.

If the user is not privileged to execute an action, an error message is shown:

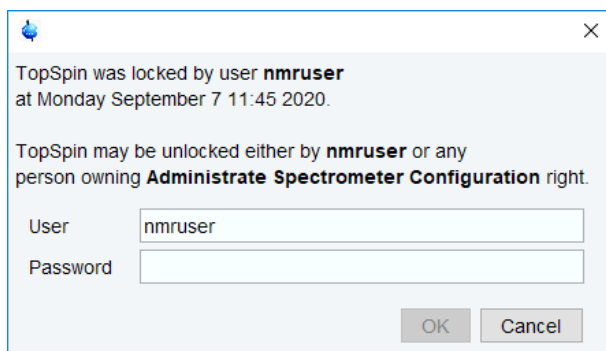
Detailed description of the user setup and available roles may be found in the Topspin GxP - Quick start guide (**Help | Manuals | Good Laboratory Practice | TopSpin GxP – Regulatory Compliance – User Manual**).

After a specified time of inactivity TopSpin can be locked automatically. The automated locking is set in **Manage Preferences | Administration Items | Automatic locking of TopSpin | Change** (Spectrometer Administration right is required).



Enter the maximum allowed idle time in minutes. Click **OK**.

Only the last logged in user or a person possessing the Spectrometer Administration right may unlock TopSpin using their respective password.



### 1.1.6 Sec. 11.10(e)

#### Extracted Text of 21 CFR Part 11

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.

**Responsibility:** Complies / System Owner

### BBIO Answer

Topspin GxP includes two different types of audit trails. Each NMR dataset contains its own audit trail. The Central Audit Trail (CAT) includes all records written to the dataset audit trails and also any system related information as user authentication or spectrometer configuration changes. The dataset audit trail is a text file protected by a hash code, and it is linked with the NMR data. For this reason, illegal manipulations of both, NMR data and the corresponding audit trail, can be detected using TopSpin command **auditcheck (Manage | Security | Show/Verify Audit Trails (audit))** and select **Verify Audit Trails** in the upcoming dialog).

If both raw and processed data are consistent, you will get the following message:

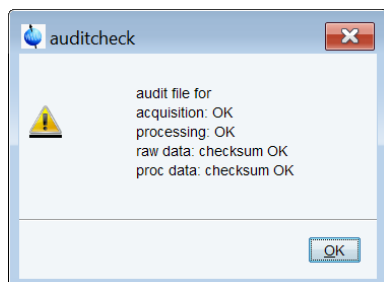


Figure 1.4: Raw and processed data are consistent.

If the data have been manipulated, e.g. with third party software or by changing certain status parameters (e.g. SI), the checksum will be inconsistent. The figure below shows the message for inconsistent processed data:

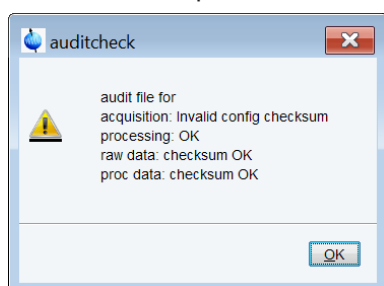


Figure 1.5: Manipulated data, checksum of acquired data invalid.

The dataset-related audit trail function is always active and cannot be switched off. There is no option (not even a hidden one) available to switch off the trail recording.

For each data manipulation, the dataset audit trail record is in the form of "WHEN / WHO / WHERE / WHAT" and this covers all functional parameters.

Enter the command **auditreport** or select **Manage | Security | Show / Verify Audit Trails** and select **Show current dataset audit trail** in the upcoming dialog, to view a human readable pdf of the respective dataset audit trail.

Audit Trail Report

Dataset Name: exam1d\_1h\_1 1 C:\Bruker\TopSpin\examdata

User: John Smith

Date: 2019-08-26 13:27:30.0353 +0200

Consistency Check:

Acquired Data Audit Log

Audit Checksum: (hash MD5) 73 90 70 98 92 13 15 c4 3c 24 9a 73 f5 3c ac 45

	WHEN	WHO	WHERE	WHAT	Explanation
1	2007-09-18 11:21:15.884 +0200	Administrator	APOLLON	created by zg, started at 2007-09-18 11:19:02.000 +0200, POWCHK enabled, PULCHK disabled	Acquisition of raw data

Processed Data Audit Log

Audit Checksum: (hash MD5) 5b ac ec 99 13 3c 4a 91 31 94 07 18 ab 72 d9 26

	WHEN	WHO	WHERE	WHAT	Explanation
1	2007-09-18 11:21:15.884 +0200	Administrator	APOLLON	created by zg, started at 2007-09-18 11:19:02.000 +0200, POWCHK enabled, PULCHK disabled	Acquisition of raw data
2	2019-07-12 12:02:43.639 +0200	INTRA-BRKR-CORP\John Smith	TITANIC	Start of raw data processing, edit LB = 5.3 FT, mod = 6 PRON = 1 PHC0 = -296.1665 PHC1 = 1.798566 SI = 32K	Exponential window mult. * FT * phase correction (110)

Figure 1.6: Human readable pdf of the dataset audit trail.

Date and time are retrieved from the PC's system clock. It is the responsibility of the system owner to protect access to the system clock on operating system level. Follow the instructions given by your operation system (e.g. "Time & Date" of MS Operating Systems).

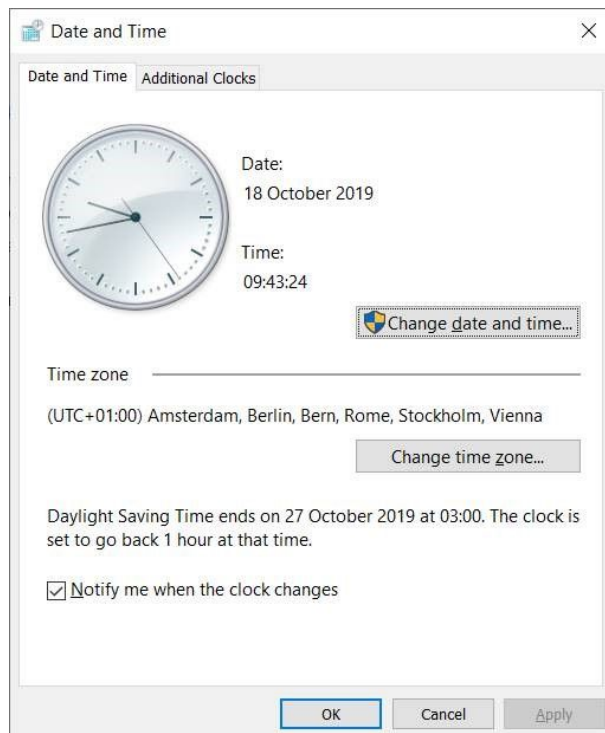


Figure 1.7: Date and time are retrieved from the PC's system clock.

The Central Audit Trail (CAT) is always activated and cannot be switched on or off when the TopSpin GxP functionality is installed. The audit records are written to a protected relational database. The CAT entries may be inspected using the Bruker CAT viewer. It may be started either from Topspin (**Manage | Security | Open CAT Viewer**), or clicking the corresponding desktop icon.

The CAT viewer requires authentication – only user owning the right "Review" can inspect the CAT. The viewer allows to apply different filters (date range, text mask for each column) to reduce the amount of shown data. The filtered records may be exported to a file in pdf format.

Brucker CAT Viewer

Central Audit Viewer

Logout

All Audit Entries

From: 6/8/2020

To: 9/8/2020

Search

Export

Reset Search Fields

Records available: 10

When	Category	Who	User Uuid	Where	Client	What	Dataset Path	Original Value	New Value
	Search for...	Search for...		Search for...	Search for...	Search for...	Search for...	Search for...	Search for...
08.09.20, 09:12:45	AUTHENTICATE	nrmuser	889a93c5-dbf0-4536-97ae-a4da9231ae0	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	login			
08.09.20, 09:12:52	CONFIGURATION	nrmuser	889a93c5-dbf0-4536-97ae-a4da9231ae0	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	expinstall Spectrometer setup			
08.09.20, 09:15:48	PROCESSING	nrmuser	889a93c5-dbf0-4536-97ae-a4da9231ae0	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	Start of raw data processing edg LB = 0.3 FT_mod = 6 PKNL = 1 PHCQ = 134.5702 PHC1 = 0.3400399 SI = 64k data hash MD5: 64k ED 24 C5 D8 34 2B 49 AE 32 9C 36 BA 26 9A 43 2F	C:/temp/GxpTest/1.1 to pspinv/GxpTest/1/pdata/1		
08.09.20, 09:15:56	PROCESSING	nrmuser	889a93c5-dbf0-4536-97ae-a4da9231ae0	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	abs ABSQ = 5 data hash MD5: 64k 55 2C 2E FA 58 34 65 E1 5D 6C 17 4B 11 3E 38 58	C:/temp/GxpTest/1.1 to pspinv/GxpTest/1/pdata/1		
08.09.20, 09:16:14	AUTHENTICATE	nrmuser	889a93c5-dbf0-4536-97ae-a4da9231ae0	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	logout			
08.09.20, 09:16:22	AUTHENTICATE	john	4d760041-d476-4771-8a7f-c6b37929b9f5	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	login			
08.09.20, 09:16:22	AUTHENTICATE	john	4d760041-d476-4771-8a7f-c6b37929b9f5	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	login			

All Rights Reserved 2020 ©Brucker BioSpin

Figure 1.8: Central Audit Viewer.

## 1.1.7 Sec. 11.10(f)

### Extracted Text of 21 CFR Part 11

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

**Responsibility:** System Owner / Support

### BBIO Answer

Each TopSpin user has assigned a role restricting the available functionality. The responsible administrator may adapt the predefined roles according the company SOPs.

## 1.1.8 Sec. 11.10(g)

### Extracted Text of 21 CFR Part 11

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.

**Responsibility:** Complies

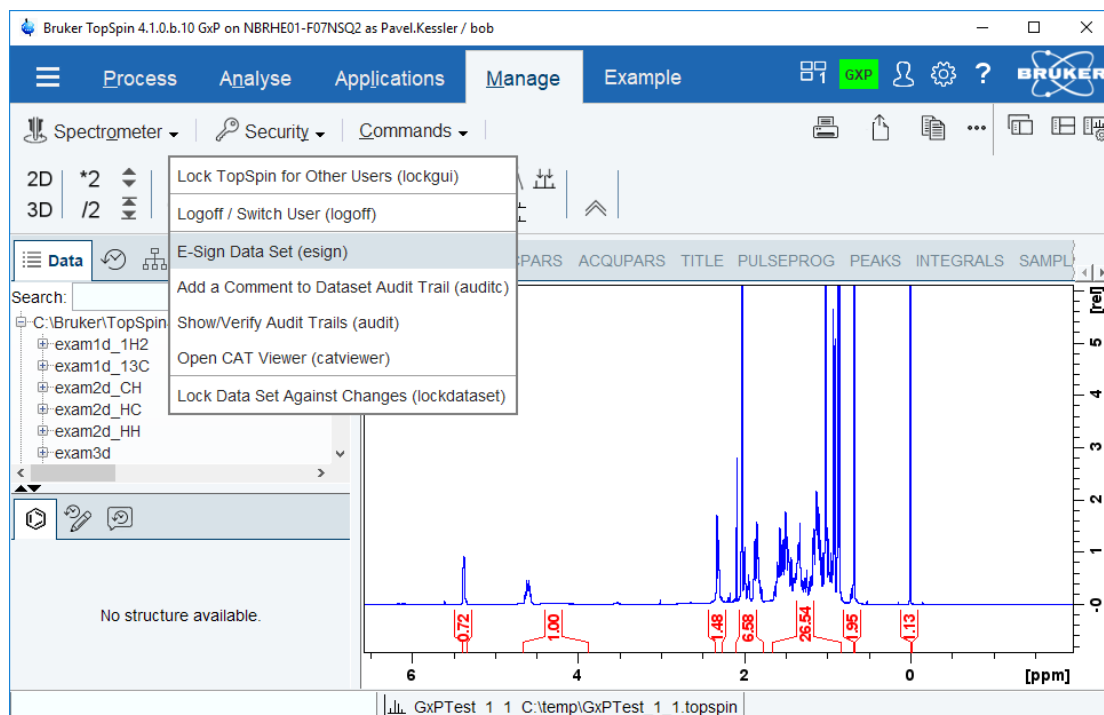
### BBIO Answer

The security features of the operating system ensure that the system can only be used by authorized individuals. See section [11.10\(d\)](#). [ 9 ]

TopSpin provides an internal user administration. See section [11.10\(d\)](#). [ 9 ]

A separate TopSpin function is used to electronically sign a data set. This function can only be executed by users registered for this purpose, and the users' password is required to validate the signature.

- Select **Manage | Security | E-Sign Data Set (esign)**



- The user must confirm his/her credentials.

- Select the appropriate signature meaning and the signed component.

The electronic signature is displayed in TopSpin. (This may be configured in Display Preferences). Electronic signatures are recorded both in the dataset audit trail and the Central Audit Trail.

When	Category	Who	User Uuid	Where	Client	What	Dataset Path	Original Value	New Value
08.09.20, 09:19:21	AUTHENTICATE	bob	4c9952e2-7d7c-44ca-8d01-7a510a13d3a3	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	login			
08.09.20, 09:19:42	APPROVAL	bob	4c9952e2-7d7c-44ca-8d01-7a510a13d3a3	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10		C:\temp\GxPTest_1_1 to pspin\GxPTest_1_1\data\	MEANING	Processed Data: Sample identity confirmed

Figure 1.9: Electronic signature recorded in CAT

Execution of any command manipulating the dataset makes the signature invalid.

## 1.1.9 Sec. 11.10(h)

### Extracted Text of 21 CFR Part 11

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

**Responsibility:** Compilies / System Owner

### BBIO Answer

Instrument tests can be run to verify the proper functionality of the spectrometer (planned maintenance and operational qualification (MRQ) Document Part Number e.g. # H184622 or H185121). Typically, Bruker Service will perform such a planned maintenance and operational qualification test as part of an annual service agreement. Refer to Bruker service offers via Bruker homepage: <https://www.bruker.com/labscape-service-and-life-cycle-support.html>

For standard operations predefined sets of parameters may be used. The system owner may define suitable tests in accordance with their routine measurements.

In Routine and Automation Operation Mode (IconNMR module) the proper set of measurement parameters for the measurement being performed is chosen automatically.

Note that the possibility to change parameters when executing functions can be prohibited.

Create an additional User account.

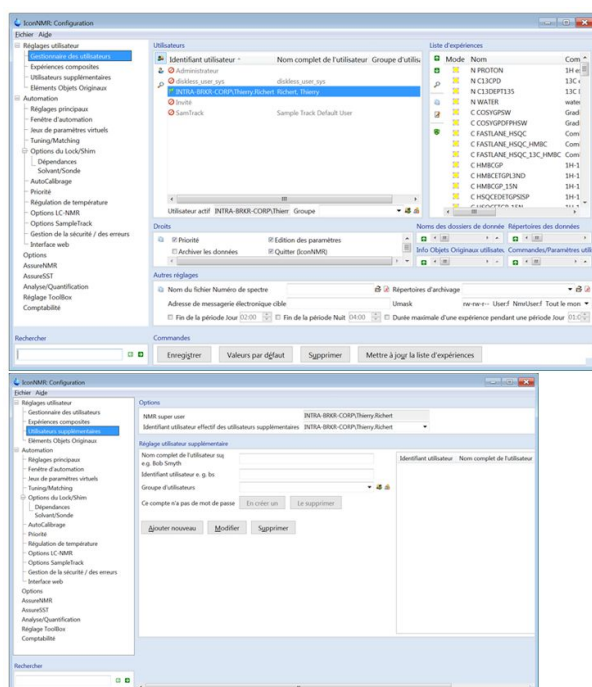


Figure 1.10: IconNMR Configuration | User Manager.

## 1.1.10 Sec. 11.10(i)

### Extracted Text of 21 CFR Part 11

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:** Complies / Support / Bruker Support

**BBIO Answer**

The Bruker software development staff consists of a group of experienced programmers, that are trained on a regular basis according to Bruker BioSpin SOPs following ISO 9001 requirements. Bruker service engineers are trained on a regular basis according to SOPs following ISO 9001 requirements. Both sets of SOPs are reviewed during internal and external audits.

Bruker offers world-wide training courses for the use of software, spectrometers and other technical equipment supplied with the system to support training of the system owner personnel. Refer to Bruker service offers via Bruker homepage: <https://www.bruker.com/en/services/training.html>

### 1.1.11 Sec. 11.10(j)

---

**Extracted Text of 21 CFR Part 11**

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:** System Owner

**BBIO Answer**

Items requested in this paragraph are the responsibility of the system owner. System Owner has to provide this information.

### 1.1.12 Sec. 11.10(k)

---

**Extracted Text of 21 CFR Part 11**

Use of appropriate controls over systems documentation including:

**Responsibility:** System Owner

### 1.1.13 Sec. 11.10(k) (1)

---

**Extracted Text of 21 CFR Part 11**

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

**Responsibility:** System Owner / Support

**BBIO Answer**

Software documentation is available in digital and printed form. Select **Help | Manuals (docs)**. A register is opened, in which the documents are stored. (The documents can also be accessed via the link below).

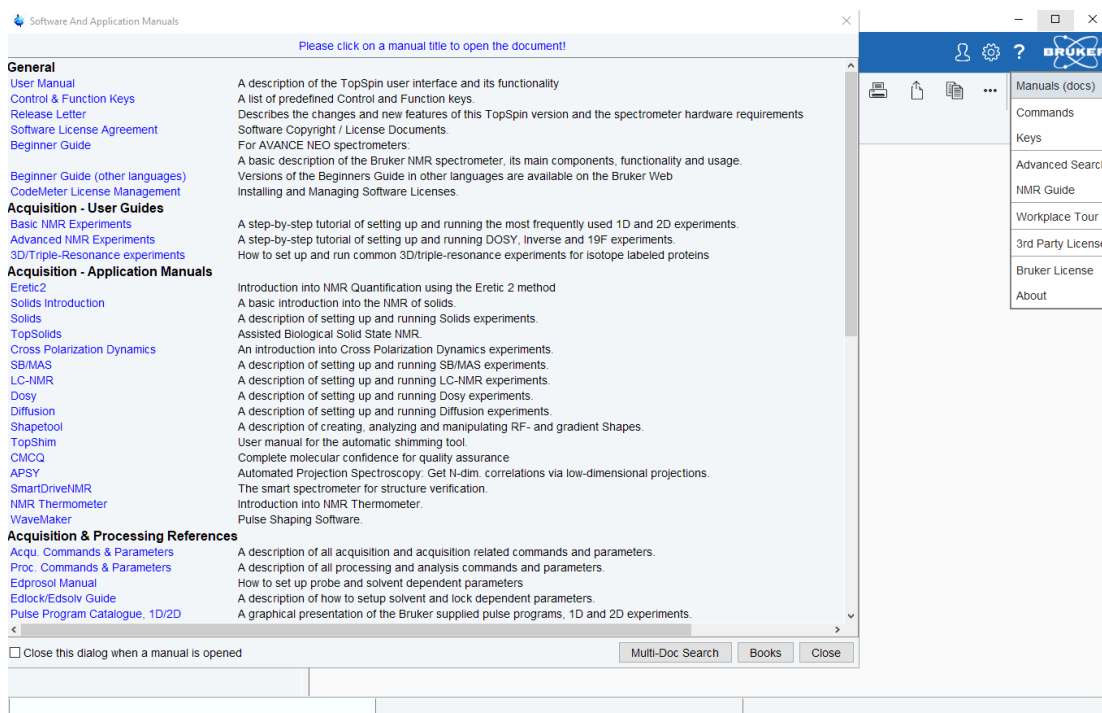


Figure 1.11: Software documentation available in TopSpin.

Refer to the Bruker Homepage under: <https://www.bruker.com/protected/en/services/user-manuals/nmr.html>

## 1.1.14 Sec 11.10(k) (2)

### Extracted Text of 21 CFR Part 11

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

**Responsibility:** Complies / System Owner / Bruker Support

### BBIO Answer

According to Bruker's SOPs, based on ISO 9001 requirements, software development is based on a software life cycle approach. This ensures that software and accompanying documentation fully conforms to the requirements of this section. See section [11.10\(e\)](#) [ 11].

New software versions will be delivered with a new set of documentation and/or documentation describing the changes of the current version compared to the previous one. See section [11.10\(k\) \(1\)](#). [ 17] New software versions do not have to be installed – installation and the time that they are installed are entirely at the discretion of the end user.



Figure 1.12: Software and Application Manuals - Release Letter.

Software and documentation are clearly identified by version numbers. All Documents provided by Bruker either electronically or in printed form contain document specific version numbers.



Figure 1.13: TopSpin document specific version number.

The TopSpin version is unequivocally identified through the version info from the TopSpin Help system.

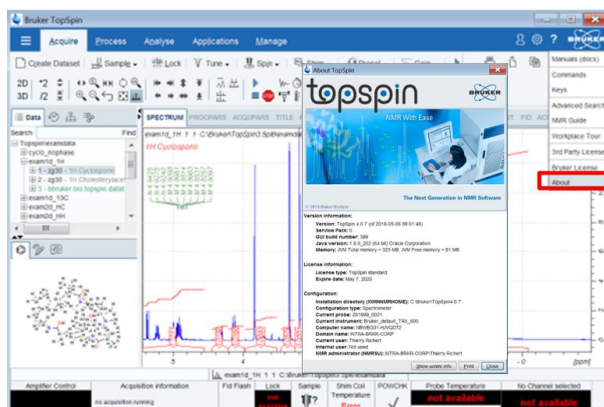


Figure 1.14: TopSpin version unequivocally identified through version info.

It is the responsibility of the system owner to establish SOPs regulating the internal handling of system documentation. System Owner has to provide this information.

## 1.1.15 Sec. 11.30 Controls for open systems

### Extracted Text of 21 CFR Part 11

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the 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 section 11.10 [ 7], as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

**Responsibility:** System Owner

### BBIO Answer

TopSpin is considered to be run in a closed system, i.e. persons working with data files need authorization to log into Windows/Linux and, if configured so, into TopSpin. If TopSpin is operated as an open system, or data are stored in an open system, it is the responsibility of the system owner to prevent unauthorized access to the data. See section 11.10(d). [ 9]

## 1.1.16 Sec. 11.50(a) Signature manifestations

### Extracted Text of 21 CFR Part 11

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

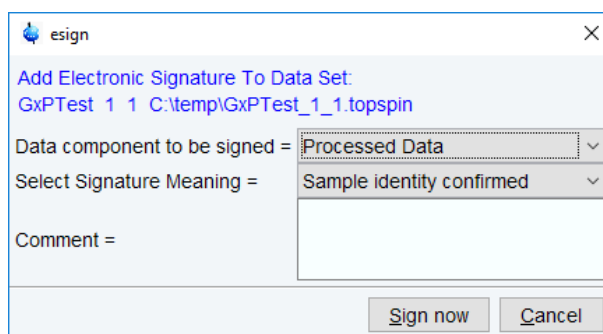
- (1) The printed name of the signer;
- (2) The date and time when the signature was executed; and
- (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

**Responsibility:** Complies

### BBIO Answer

All required information is automatically added to the electronic signature and stored in audit trails.

The meaning of the signature can be chosen from a list of possible meanings. The list is set up by the IM administrator. Different meanings can be specified for each signer.



## 1.1.17 Sec. 11.50(b) Signature manifestations

### Extracted Text of 21 CFR Part 11

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).

**Responsibility:** Complies

**BBIO Answer**

Electronic signatures are an integral part of the Central Audit Trail which records all user operations. This is a database with export capabilities for files in pdf format. Signatures are also recorded in the dataset audit trails.

The display and printout (plot) of the data may also include the signatures.

## 1.1.18 Sec. 11.70 Signature / record linking

---

**Extracted Text of 21 CFR Part 11**

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.

**Responsibility:** Complies

**BBIO Answer**

Electronic signatures are stored in the respective audit trails. See section [Sec. 11.50\(a\) Signature manifestations](#) [▶ 20] and [11.50\(b\)](#). [▶ 20]

Signatures cannot be deleted, changed, overwritten or copied to another data file. If a user were able to make such changes, for example by using different software, then that manipulation would make a data set inconsistent. Such an inconsistency would be detected using the respective TopSpin consistency check function. See section [11.10\(e\)](#). [▶ 11]

## 1.2 Subpart C - Electronic Signatures

---

Subpart C – Electronic Signatures<sup>2</sup>

### 1.2.1 Sec. 11.100 General requirements

---

### 1.2.2 Sec. 11.100(a)

---

#### **Extracted Text of 21 CFR Part 11**

Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

**Responsibility:** Complies

#### **BBIO Answer**

Electronic signatures require authentication of the signer. This is provided by Topspin user management and signatures are therefore clearly assigned to identity of individuals.

Duplicate user IDs cannot be entered. A user is uniquely identified by his User ID (UUID). A user account may be deleted by an authorized user (for example if an employee leaves the organization) and at some time in the future, a new user account with the same user name could be created. Nevertheless, users will be differentiated by their UUID.

### 1.2.3 Sec. 11.100(b)

---

#### **Extracted Text of 21 CFR Part 11**

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:** System Owner

#### **BBIO Answer**

The IM administrator shall assign the appropriate (e.g. Assay Verifier) roles to each Topspin user eligible for signing data set. The corresponding signature meaning(s) should be also set.

---

<sup>2</sup> Revised as of April 1, 2016

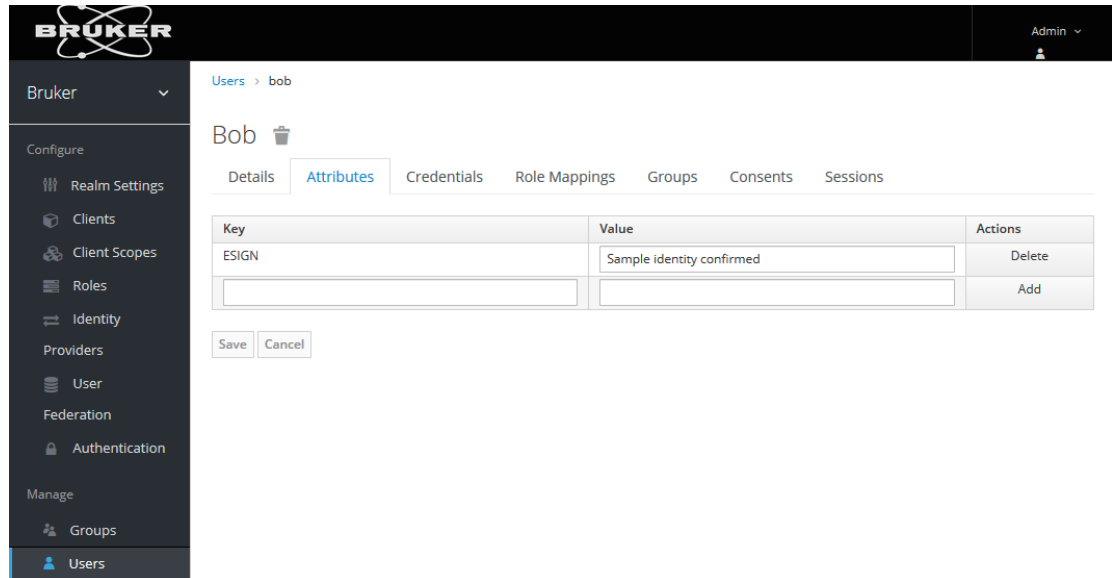


Figure 1.15: Meaning of electronic signature may be set in the IM console (Keycloak).

#### 1.2.4 Sec. 11.100(c)

##### Extracted Text of 21 CFR Part 11

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.

**Responsibility:** System Owner

##### BBIO Answer

The system owner is responsible for providing these controls and assurances.

#### 1.2.5 Sec. 11.100(c) (1)

##### Extracted Text of 21 CFR Part 11

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.

**Responsibility:** System Owner

##### BBIO Answer

The system owner is responsible for these certificates.

#### 1.2.6 Sec 11.100(c) (2)

##### Extracted Text of 21 CFR Part 11

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:** System Owner

##### BBIO Answer

The system owner is responsible for these certificates.

### 1.2.7 Sec. 11.200 Electronic signature components and controls

---

### 1.2.8 Sec. 11.200 (a)

---

#### Extracted Text of 21 CFR Part 11

Electronic signatures that are not based upon biometrics shall: ...

### 1.2.9 Sec. 11.200(a) (1)

---

#### Extracted Text of 21 CFR Part 11

Employ at least two distinct identification components such as an identification code and password.

**Responsibility:** Complies

#### BBIO Answer

To execute a signature, input of a user ID and a password is required. See section [11.10\(g\)](#) [\[ 14\]](#).

Duplicate User IDs are prohibited. See section [11.10\(d\)](#). [\[ 9\]](#)

### 1.2.10 Sec. 11.200(a) (1i)

---

#### Extracted Text of 21 CFR Part 11

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.

**Responsibility:** Complies

#### BBIO Answer

The electronic signature is only possible for the user who is signed in TopSpin. The user name for signature is set by default and cannot be changed, the password must be entered for each electronic signature

### 1.2.11 Sec. 11.200(a) (1ii)

---

#### Extracted Text of 21 CFR Part 11

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.

**Responsibility:** Complies

#### BBIO Answer

When TopSpin is restarted, or if the active user is changed within a TopSpin session, a new "continuous period of controlled system access" begins and both the user ID and the password have to be re-entered to log in. The user name for signature is set by default and cannot be changed, the password must be entered for each electronic signature.



**1.2.12 Sec. 11.200(a) (2)**

---

**Extracted Text of 21 CFR Part 11**

Be used only by their genuine owners; and ...

**Responsibility:** System Owner

**BBIO Answer**

The system owner must provide appropriate SOPs.

**1.2.13 Sec. 11.200(a) (3)**

---

**Extracted Text of 21 CFR Part 11**

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.

**Responsibility:** System Owner

**BBIO Answer**

The system owner must provide appropriate SOPs.

**1.2.14 Sec. 11.200(b)**

---

**Extracted Text of 21 CFR Part 11**

Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

**Responsibility:** n/a (does not apply)

**BBIO Answer**

TopSpin uses the combination of User ID and password for authorization check. Biometric devices are not supported. See section [11.10\(d\)](#) [ 9].

**1.2.15 Sec. 11.300 Controls for identification codes/passwords**

---

**Extracted Text of 21 CFR Part 11**

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: ...

**1.2.16 Sec. 11.300(a)**

---

**Extracted Text of 21 CFR Part 11**

Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

**Responsibility:** System Owner / Support

**BBIO Answer**

The Electronic Signature function of TopSpin does not accept duplicate user UUIDs. This guarantees that the combination of User ID and password will be unique on a system.

The user UUID, which is unique, is set automatically when defining a new user. the actual user name and password are not checked for duplicate name. Due to security reasons TopSpin does not check for duplicate passwords.

### 1.2.17 Sec. 11.300(b)

---

#### **Extracted Text of 21 CFR Part 11**

Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

**Responsibility:** System Owner / Complies

#### **BBIO Answer**

The system owner is responsible for these checks and reviews.

Password aging of TopSpin internal users can also be set to make it consistent with the relevant customer specific SOP.

For users who are no longer active in the system (for example if they leave the company) then their accounts are set to inactive. Their records are still held but they can no longer access the TopSpin system.

### 1.2.18 Sec. 11.300(c)

---

#### **Extracted Text of 21 CFR Part 11**

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.

**Responsibility:** System Owner

#### **BBIO Answer**

Each user account may be disabled in the IM console (Keycloak).

TopSpin does not support the use of hardware (e.g. tokens) for authentication.

### 1.2.19 Sec. 11.300(d)

---

#### **Extracted Text of 21 CFR Part 11**

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.

**Responsibility:** System Owner

#### **BBIO Answer**

All attempts to authenticate (this includes either login or electronic signature) are logged in the Central Audit Trail. The authentication failures are also logged. The complete history can be reviewed by opening the CAT viewer, enter **AUTHENTICATE** in the **Category**, click **Search**. The CAT viewer will show the relevant information:

From: 6/9/2020	To: 9/9/2020	<input type="button" value="Search"/> <input type="button" value="Export"/> <input type="button" value="Reset Search Fields"/>				
When	Category	Who	User Uuid	Where	Client	What
	AUTHE	Search for...	Search for...	Search for...	Search for...	Search for...
08.09.20, 09:12:45	AUTHENTICATE	nmruser	889a93c5-dbf0-4536-97ae-af4da9231ae0	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	login
08.09.20, 09:16:14	AUTHENTICATE	nmruser	889a93c5-dbf0-4536-97ae-af4da9231ae0	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	logoff
08.09.20, 09:16:22	AUTHENTICATE	john	4d760041-d476-4771-8a7f-ce837929bfff5	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	login
08.09.20, 09:17:08	AUTHENTICATE	john	4d760041-d476-4771-8a7f-ce837929bfff5	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	logoff
08.09.20, 09:17:12	AUTHENTICATE	bob		NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	Login failed Invalid credentials
08.09.20, 09:19:21	AUTHENTICATE	bob	4ca952e2-7d7c-44ca-8d0f-7ad10a13d3a3	NBRHE01-F07NSQ2	TopSpin 4.1.0.b.10	login

## 1.2.20 Sec. 11.300(e)

### Extracted Text of 21 CFR Part 11

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.

**Responsibility:** n/a (does not apply)

### BBIO Answer

TopSpin uses the combination of User ID and password for authorization check. See section [11.10\(d\)](#). [ 9]



## 2 Appendix A

*Revised as of October 4, 2018*

### **21 CFR Part 11: Electronic Records; Electronic Signatures**

#### **Subpart A: General Provisions**

##### **Sec. 11.1 Scope**

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(g) This part does not apply to electronic signatures obtained under 101.11(d) of this chapter.

(h) [Reserved]

(i) This part does not apply to records required to be established or maintained by part 117 of this chapter. Records that satisfy the requirements of part 117 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(j) This part does not apply to records required to be established or maintained by part 507 of this chapter. Records that satisfy the requirements of part 507 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(k) This part does not apply to records required to be established or maintained by part 112 of this chapter. Records that satisfy the requirements of part 112 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(l) This part does not apply to records required to be established or maintained by subpart L of part 1 of this chapter. Records that satisfy the requirements of subpart L of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(m) This part does not apply to records required to be established or maintained by subpart M of part 1 of this chapter. Records that satisfy the requirements of subpart M of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(n) This part does not apply to records required to be established or maintained by subpart O of part 1 of this chapter. Records that satisfy the requirements of subpart O of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(o) This part does not apply to records required to be established or maintained by part 121 of this chapter. Records that satisfy the requirements of part 121 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

### Sec. 11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

1. The requirements of this part are met;
2. The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

### Sec. 11.3 Definitions

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

1. **Act** means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).
2. **Agency** means the Food and Drug Administration.
3. **Biometrics** means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
4. **Closed system** means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
5. **Digital signature** means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
6. **Electronic record** means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

7. **Electronic signature** means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
8. **Handwritten signature** means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.
9. **Open system** means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

**Authority:** 21 U.S.C. 321-393; 42 U.S.C. 262.

**Source:** 62 FR 13464, Mar. 20, 1997, unless otherwise noted.





### 3 Appendix B

#### Short comparison of FDA 21 CFR 11 to EU Eudralex Vol.4 – Annex 11 requirements towards electronic records and computerized systems

Requirements of **EudraLex – Volume 4 – Good Manufacturing Practice (GMP) guidelines**:

**Annex 11 – Computerized Systems** (revision January 2011) are also taken into consideration in this manual!

Eudralex guidelines impact manufacturers in the EU and those who export to the EU markets.

Close scrutiny of the parallel **FDA (21 CFR part11)** and **EU rules (Eudralex – Vol.4 – Annex 11)** shows, the authorities share a mutual intent to have safe, validated computer systems and qualified networks for drug and device manufacturing on both markets. The systematic comparison chart below shows that both rules and guidelines are substantially equivalent in their requirements.

Limited areas of **Part 11** in comparison to **Annex 11** are dissimilar; these, for the most part, are limited to the verification of identity and accountability of actions by authorized individuals, as well as to the reporting to authorities.

**Part 11** applies to e-submissions to the FDA. **Annex 11** is in that perspective different from **Part 11** in that it takes a risk management approach to criticality and emphasizes a systems approach to periodic evaluations.



**Annex 11** is more a 'how to' while **Part 11** is 'thou shalt' in tone.

Together they form a robust and usable guide for computer validation professionals leading their companies and clients to compliance.

	FDA 21 CFR Part 11 USA	Eudralex Vol.4 – Annex 11 EU
Scope / Principle	Electronic records and electronic signatures as used for all FDA regulated activities.	Computerized systems as part of GMP regulated activities. Application should be validated. IT infrastructure should be qualified.
Focus	Using electronic records and signatures in open and closed computer systems.	Risk-based quality management of computerized systems.
Objective	Electronic records and signatures should be as trustworthy and reliable as paper records and handwritten signatures.	Using a computerized system should ensure the same product quality and quality assurance as manual systems with no increase in the overall risk.

FDA 21 CFR Part 11 USA		Eudralex Vol.4 – Annex 11 EU	
Section No.	Title	Paragraph	Cross Reference
<b>11.10</b>	<b>Subpart B--Electronic Records</b>		<b>Computerized Systems</b>
<a href="#">11.10 (a)</a> <a href="#">[ 7]</a>	Validation	4	Validation
<a href="#">11.10 (b)</a> <a href="#">[ 7]</a>	Generate accurate and complete copies	8.1	Printouts
<a href="#">11.10 (c)</a> <a href="#">[ 8]</a>	Protection of records for accurate retrieval	7 12 17	Data Storage Security Archiving
<a href="#">11.10 (d)</a> <a href="#">[ 9]</a>	Limiting system access to authorized individuals	7.1 10 12.1	Secured and accessible Change and Configuration Management Security, physical/logical
<a href="#">11.10 (e)</a> <a href="#">[ 11]</a>	Record of operator entries (audit trail)	7.1 9 10 12.4 14(c)	Secured and accessible Audit Trails Change and Configuration Management Data management/operators entries Electronic Signature
<a href="#">11.10 (f)</a> <a href="#">[ 14]</a>	Operational system checks	5 6	Data Accuracy Checks
<a href="#">11.10 (g)</a> <a href="#">[ 14]</a>	Authority checks	7.1 12.1	Secured and accessible Security, physical/logical
<a href="#">11.10 (h)</a> <a href="#">[ 16]</a>	Device checks	4.8	Validation
<a href="#">11.10 (i)</a> <a href="#">[ 16]</a>	Personnel (who develop, users and maintain systems)	2	Personnel
<a href="#">11.10 (j)</a> <a href="#">[ 17]</a>	User accountability for actions initiated under e-signatures	—	not covered
<a href="#">11.10 (k)</a> <a href="#">[ 17]</a>	Documentation control	4.2 9 10 —	Change control and deviations Audit Trails Change and Configuration Management Periodic evaluation
<a href="#">11.30</a> <a href="#">[ 20]</a>	Controls for open systems	5	Principle (all systems) Data
11.50	Signature manifestations	14	Electronic Signature
<a href="#">11.70</a> <a href="#">[ 21]</a>	Signature/record linking	14(b)	Electronic Signature
<b>11.100</b>	<b>General requirements</b>	—	—
<a href="#">11.100 (a)</a> <a href="#">[ 22]</a>	Unique/not reused	—	not covered

<b>11.100</b>	<b>General requirements</b>	—	—
<a href="#">11.100 (b)</a> <a href="#">[▶ 22]</a>	Verify identity	—	not covered
<a href="#">11.100 (c)</a> <a href="#">[▶ 23]</a>	Certify equivalent to handwritten	14 (a)	same as hand-written
<b>11.200</b>	<b>Electronic signature components and controls</b>	—	—
<a href="#">11.200 (a)</a> <a href="#">[▶ 24]</a>	Not based on biometrics	12.1	Security, physical/logical
<a href="#">11.200 (b)</a> <a href="#">[▶ 25]</a>	Based on biometrics	12.1	Security, physical/logical
<b>11.300</b>	<b>Controls for identification codes/ passwords</b>	—	—
<a href="#">11.300 (a)</a> <a href="#">[▶ 25]</a>	Unique	12.1	Security, physical/logical
<a href="#">11.300 (b)</a> <a href="#">[▶ 26]</a>	Periodically checked	11 12.3	Periodic Evaluation Security- record events
<a href="#">11.300 (c)</a> <a href="#">[▶ 26]</a>	Procedures to deauthorize	12.3	Security, record events
<a href="#">11.300 (d)</a> <a href="#">[▶ 26]</a>	Prevent unauthorized use	12.1	Security
<a href="#">11.300 (e)</a> <a href="#">[▶ 27]</a>	Proper function	11	Periodic evaluation



# Revision History

Version	Date	Change Reason
001	18.09.2020	Introduction of TopSpin GxP with TopSpin 4.1.0 – update of 21 CFR Part 11 Compliance Document
002	05.10.2021	Updated documentation of TopSpin GxP user management with TopSpin 4.1.4



---

Note: Changes to this document, as documented above, always apply to the latest released version and patch level (pl) of TopSpin NMR Software available at the time of publishing.

---



## 4 Contact

### Manufacturer

Bruker BioSpin GmbH  
Rudolf-Plank-Str. 23  
D-76275 Ettlingen  
Germany

E-Mail: [nmr-support@bruker.com](mailto:nmr-support@bruker.com)  
<http://www.bruker.com>  
WEEE DE43181702

### Bruker BioSpin Hotlines

Contact our Bruker BioSpin service centers.

Bruker BioSpin provides dedicated hotlines and service centers, so that our specialists can respond as quickly as possible to all your service requests, applications questions, software or technical needs.

Please select the service center or hotline you wish to contact from our list available at:

<https://www.bruker.com/service/information-communication/helpdesk.html>





# List of Figures

Figure 1.1:	JCAMPDX.....	8
Figure 1.2:	Lock Data Set Against Changes .....	9
Figure 1.3:	Microsoft Operating System Account. ....	9
Figure 1.4:	Raw and processed data are consistent.....	12
Figure 1.5:	Manipulated data, checksum of acquired data invalid. ....	12
Figure 1.6:	Human readable pdf of the dataset audit trail. ....	12
Figure 1.7:	Date and time are retrieved from the PC's system clock. ....	13
Figure 1.8:	Central Audit Viewer. ....	14
Figure 1.9:	Electronic signature recorded in CAT .....	15
Figure 1.10:	IconNMR Configuration   User Manager.....	16
Figure 1.11:	Software documentation available in TopSpin.....	18
Figure 1.12:	Software and Application Manuals - Release Letter.....	19
Figure 1.13:	TopSpin document specific version number. ....	19
Figure 1.14:	TopSpin version unequivocally identified through version info. ....	19
Figure 1.15:	Meaning of electronic signature may be set in the IM console (Keycloak). ....	23







**Bruker Corporation**

[info@bruker.com](mailto:info@bruker.com)  
[www.bruker.com](http://www.bruker.com)



Part No: H181366