NMR in Pharma: Application of Data Integrity Principles

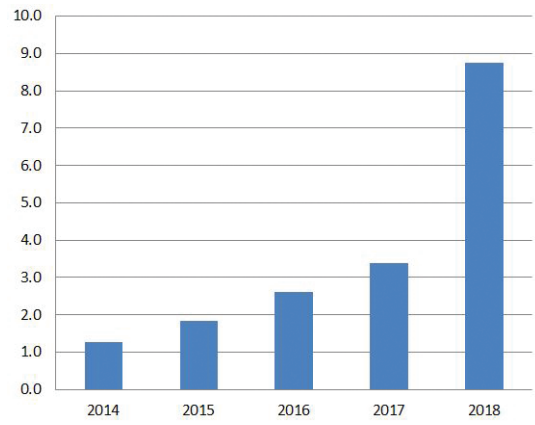
Ian Clegg, Regional Market Manager
Bruker BioSpin

Data Integrity (DI) principles are important to all those who generate, or use data because they underpin confidence in the data obtained and also in any conclusions drawn. Whatever the setting it is important, for example, to ensure that data has been obtained correctly by suitably qualified personnel using calibrated and maintained instruments and that the data has been stored in its raw form as well as with the metadata that unambiguously describes how it has been processed.

Within the Pharma sector, the principles of DI have special status due to the fact that adherence is mandated by the industry regulators but primarily because the underlying reason is that non-adherence can lead to the loss of efficacy of pharmaceutical products and/or can cause its safety profile to be compromised: both these possibilities have serious negative consequences for patients.

It is clear that DI principles are routinely applied to all scientific instruments that are employed within this sector. Despite some notable exceptions (especially the well-established use of NMR to determine the potency of reference materials[1] as well as the widely employed process of structural elucidation / verification), NMR has tended not to be involved too directly in late stage pharmaceutical development and manufacture. The requirement to adhere to the principles of DI have therefore been relatively infrequent. However, this position is set to change due in part to the significant recent interest in applications such as qNMR for the determination of potency of finished products. Also, adherence to DI principles seems to be a strong general focus of the regulatory agencies recently: an analysis of warning letters issued by US FDA[2] is shown in Figure 1. This figure shows the percentage of all warning letters issued during each year (Jan to early Aug, for 2018) that

Figure 1

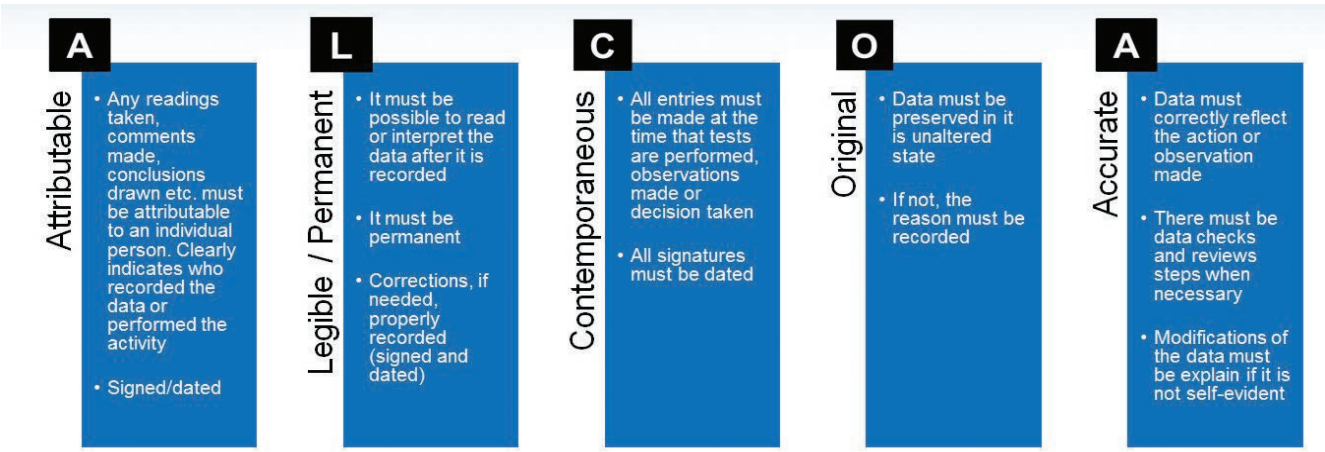


contain at least one specific finding about non-compliance with DI principles. The steady increase of the years is obvious, and overall it is clear that NMR applications will increasingly be scrutinised for adherence to DI principles.

An NMR method follows the generic stages of acquisition of an FID, followed by a Fourier transform then baseline correction etc. are performed and finally, resonance peaks are integrated and a result is calculated. This is the same as other techniques, for example a Mid-IR method follows the stages of acquisition of an interferogram, followed by a Fourier transform, then baseline correction etc. are performed and finally, absorbance peaks are integrated and a result is calculated. It is clear therefore that from the point of view of DI principles, NMR is identical to other analytical techniques.

There are several sets of relevant regulations and standards for example from the MHRA[3] and the FDA[4]. The acronym ALCOA (Figure 2) and its derivative ALCOA+ are well known and serve as a useful summary of the principles.

Figure 2



Data Integrity Implementation

Examples of methods by which a pharmaceutical company who uses NMR in GxP environments can show that they adhere to the principles of DI are shown in a series of figures, which in turn are drawn from existing Bruker software programs:

Figure 3 shows how GxP supportive features are enabled. Once a user takes the conscious decision that they are operating under GxP and the software is installed then the configuration cannot be undone. This feature underpins most of the principles of ALCOA.

Figure 3

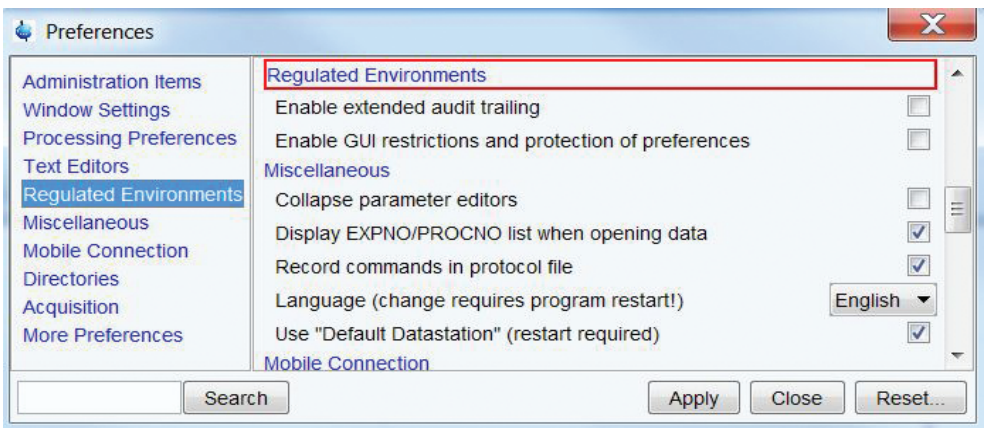


Figure 4 shows how datasets are locked post acquistion and this feature illustrates compliance with principle of “Original”.

Figure 4

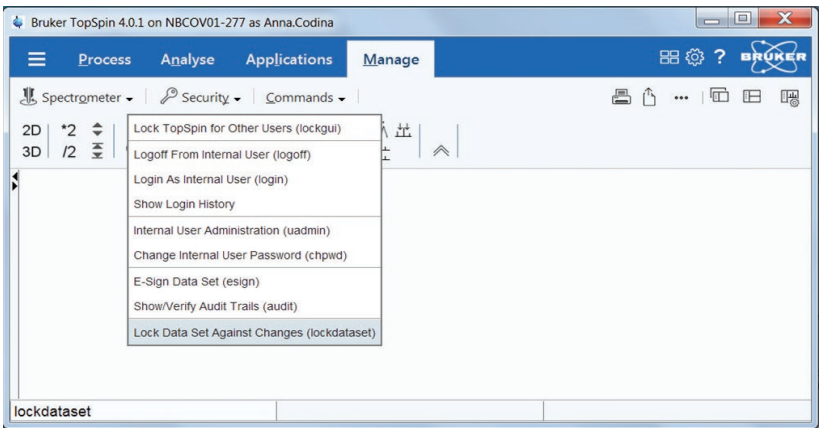
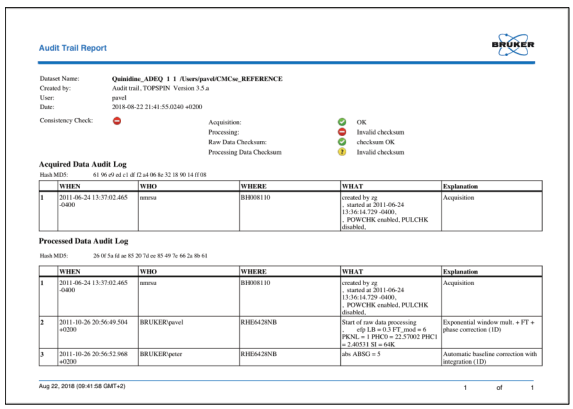


Figure 5 shows a brief example of an audit file. During operation in GxP mode, information is continually being added to this file and it supports the principles of Attributable (since, the user is clearly indicated) and time stamps support the principle of “Contemporaneous”. Additionally, this audit file is protected by a MD5 checksum.

Figure 5

```
##TITLE= Audit trail, TOPSPIN                    Version 3.5.a
##JCAMPDX= 5.01
##ORIGIN= Bruker BioSpin GmbH
##OWNER= pavel
$$ c:\pavel\data\NKK/Quinidine_CMCse_June2011/1/pdata/1/auditp.txt
##AUDIT TRAIL=  $$ (NUMBER, WHEN, WHO, WHERE, PROCESS, VERSION, WHAT)
(   1,<2011-06-24 13:37:02.465 -0400>,<nmrsu>,<BH008110>,<go>,<TOPSPIN 3.0>,
     <created by zg
          started at 2011-06-24 13:36:14.729 -0400,
          POWCHK enabled, PULCHK disabled,
      configuration hash MD5:
      AA 31 EF 65 98 C3 D4 C2 22 21 F5 BF F1 DB 53 CD
      data hash MD5: 64K
      62 CE 9D A5 16 7C 38 86 DA 3C C8 85 34 6F D6 FD>)
(   2,<2011-10-26 20:56:49.504 +0200>,<BRUKER\pavel>,<RHE6428NB>,<proc1d>,<TOPSPIN 3.5.a>,
     <Start of raw data processing
      efp LB = 0.3 FT_mod = 6 PKNL = 1 PHC0 = 22.57002 PHC1 = 2.40531 SI = 64K
      data hash MD5: 64K
      9D 75 5B 11 B1 FD 25 59 AC 15 D8 6A 94 E5 97 7E>)
(   3,<2011-10-26 20:56:52.968 +0200>,<BRUKER\peter>,<RHE6428NB>,<proc1d>,<TOPSPIN 3.5.a>,
     <abs ABSG = 5
      data hash MD5: 64K
      90 53 C3 BD 64 B9 9C 3C 23 CE 8D 9C F6 7D E1 E8>)
##END=

$$ hash MD5
$$ 26 0F 5A FD AE 85 20 7D EE 85 49 7E 66 2A 8B 61
```


Audit Trail Report

Dataset Name: Quinidine_ADEQ 1 1 /Users/pavel/CMCse_REFERENCE
Created by: Audit trail, TOPSPIN Version 3.5.a
User: pavel
Date: 2018-08-22 21:41:55.0240 +0200
Consistency Check:

Acquisition: OK
Processing: Invalid checksum
Raw Data Checksum: checksum OK
Processing Data Checksum: Invalid checksum

Acquired Data Audit Log
Hash MD5: 61 96 d9 ad c1 df f2 a4 06 8c 32 18 90 14 f1 08

	WHEN	WHO	WHERE	WHAT	Explanation
1	2011-06-24 13:37:02.465 -0400	nmrsu	BH008110	created by zg , started at 2011-06-24 13:36:14.729 -0400, , POWCHK enabled, PULCHK disabled,	Acquisition

Processed Data Audit Log
Hash MD5: 26 0f 5a fd ae 85 20 7d ee 85 49 7e 66 2a 8b 61

	WHEN	WHO	WHERE	WHAT	Explanation
1	2011-06-24 13:37:02.465 -0400	nmrsu	BH008110	created by zg , started at 2011-06-24 13:36:14.729 -0400, , POWCHK enabled, PULCHK disabled,	Acquisition
2	2011-10-26 20:56:49.504 +0200	BRUKER\pavel	RHE6428NB	Start of raw data processing efp LB = 0.3 FT_mod = 6 PKNL = 1 PHC0 = 22.57002 PHC1 = 2.40531 SI = 64K	Exponential window mult. + FT + phase correction (1D)
3	2011-10-26 20:56:52.968 +0200	BRUKER\peter	RHE6428NB	abs ABSG = 5	Automatic baseline correction with integration (1D)

Aug 22, 2018 (09:41:58 GMT+2) 1 of 1

Figure 6 shows an example of robust user access control, and supports the more general requirement to clearly control access to the software system.

Figure 6

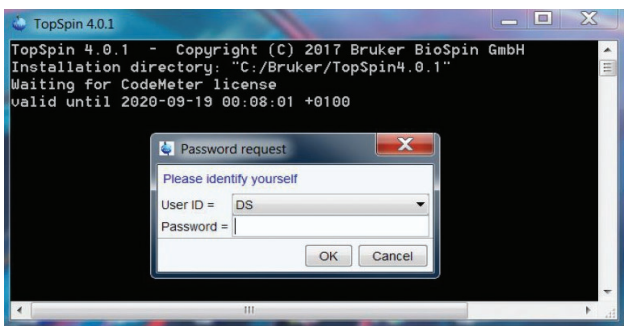
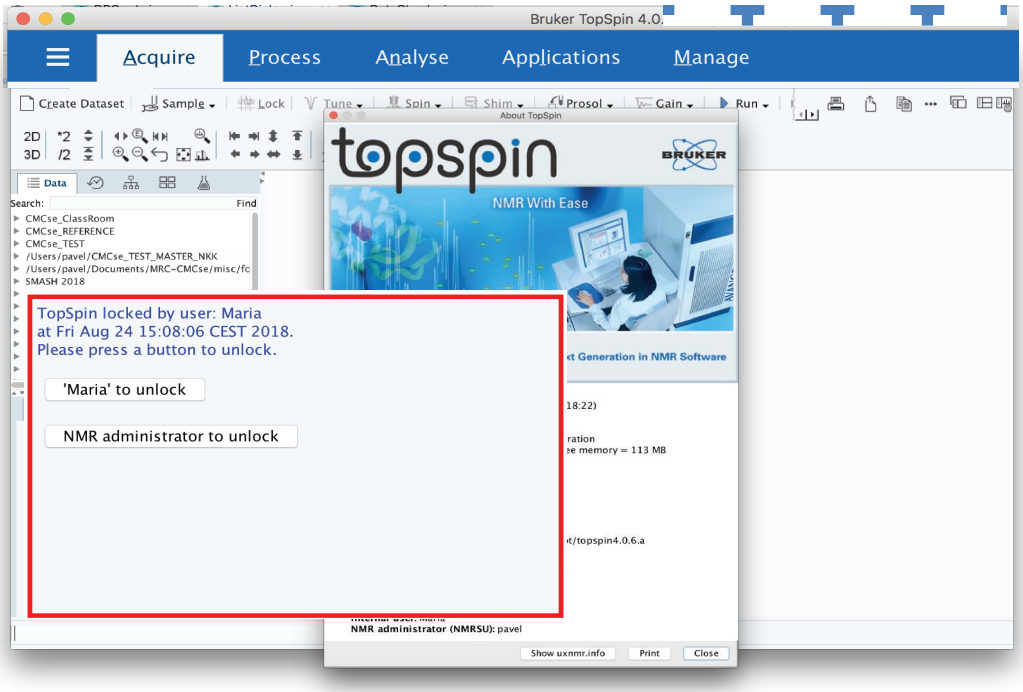


Figure 7 shows an example of the spectrometer interface that has been locked by a user.

Figure 7



Conclusions

In summary, it is anticipated that NMR systems and methods used within Pharma, will be the subject of significantly more scrutiny with respect to DI. Companies who employ this technology will be expected, for example, to show that there is robust user access control, that raw data sets are fully protected, that data treatment sequences are clearly available, that data outputs (e.g. spectra, and numerical outputs) accurately reflect what has happened. The brief series of vignettes presented in this paper are examples of how Bruker BioSpin software can help customers achieve compliance with principles of data Integrity.

Additionally, it will be expected the instruments have been properly qualified i.e. designed, installed, commissioned, operated and maintained… but the requirements for instrument qualification are an additional matter.

References:

1. Webster,G.K., and Kumar, S., Anal.Chem., 2014, 86, 11474-11480
2. https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/. Accessed 22Aug18
3. MHRA Discussion Document on DI https://www.gov.uk/government/publications/guidance-on-gxp-data-integrity. Accessed 22Aug18
4. FDA Reference Document on 21CFRpt11 https://www.fda.gov/downloads/regulatoryinformation/guidances/ucm125125.pdf. Accessed 22Aug18

www.bruker.com ● **Bruker BioSpin**
info@bruker.com