MHRA Data Integrity Guidance, 2015 and 2018

MHRA published a revision to their 2015 Data Integrity Guidance, finalizing the draft revision published for consultation in 2016. The MHRA Inspectorate blog says that the health authority received over 1300 comments during the consultation process. The revision was a coordinated effort among the GCP, GDP, GLP, GMP and GPvP inspection groups reflecting a broad source of input. MHRA specifically, however, excluded devices from the scope of this guidance. Regarding alignment with guidance from other health authorities, MHRA states: “The GXP data integrity guidance has a high degree of alignment with documents published by other regulators such as PIC/S, WHO, OECD (guidance and advisory documents on GLP) and EMA. It is designed to facilitate compliance through education, whilst clarifying the MHRA’s position on data integrity and the minimum expectation to achieve compliance.”

The MHRA guidance and WHO guidance scope includes the entirety of GXP. The PIC/S guidance on the same topic addresses GMP and GDP, the EMA and FDA guidance address GMP although the principles are relevant to GXP.

CHANGES, REVISIONS, and DELETIONS from the 2015 VERSION:

The 2018 revision of the MHRA Guidance on Data Integrity and Definitions, in general, provides more detail and granularity than the 2015 version. Several items from the 2015 version are absent from the 2018 version. Similarly, MHRA includes new topics or significantly increased detail in the 2018 version. We address all below and identify the nature of the addition, deletion or revision. Sections are addressed in the order they appear in the guidance. “ADDITIONS” are those sections that are new in 2018, “REVISIONS” generally denote expansion of sections between the two versions and “DELETED” identifies sections in the 2015 guidance that did not carry over to the 2018 version. We group the type of changes together within the two divisions in the document. Items are grouped in these three categories.

<table>
<thead>
<tr>
<th>NATURE OF CHANGE</th>
<th>CHANGE DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PRINCIPLES, CRITICALITY, RISK AND SYSTEM DESIGN</strong></td>
<td></td>
</tr>
<tr>
<td><strong>DELETION</strong></td>
<td>Figure 1 in the 2015 version shows the spectrum of simple to complex computerized systems. It has been removed in the 2018 version. The text in section 4.3 of the 2018 version provides a narrative version of the 2015 Figure 1. The 2016 draft guidance included the figure and thus it was removed as an outcome of the consultation process.</td>
</tr>
<tr>
<td><strong>ADDITION</strong></td>
<td>The scope of the 2015 guidance was limited to GMP, the scope of the 2018 version includes GCP, GLP, GMP for pharmaceuticals and excludes consideration of devices. Reference is made to the Introduction section of the guidance. The introduction section is largely new in this revision and does not reflect information in the 2015 publication.</td>
</tr>
<tr>
<td><strong>ADDITION</strong></td>
<td>The Principles of Data Integrity section introduces the acronym DIRA, Data Integrity Risk Assessment. Many of the ten principles consolidated in this section reflect requirements that are previously found throughout the earlier document but are consolidated in the 2018 version.</td>
</tr>
<tr>
<td>REVISION</td>
<td>The 2015 version included a section titled “Establishing Data Criticality and Inherent Integrity Risk” that is substantially expanded with new text and detail in the 2018 version. Additional detail is provided in examples that is welcome.</td>
</tr>
<tr>
<td>REVISION</td>
<td>Section 5.0 titled “Designing Systems and Processes” in the 2018 version has also been substantially expanded over the 2015 version. It addresses a GLP example where scribes record activities, such as for necropsies.</td>
</tr>
<tr>
<td>REVISION</td>
<td>The format is revised from a tabulation format that included terms, definitions and expectations/guidance (where relevant) in 2015 to a non-tabulated narrative format in 2018.</td>
</tr>
</tbody>
</table>

**DEFINITIONS and INTERPRETATIONS**

| DELETION | The revised definition of ‘Raw Data’ in section 6.2 does not include the potential for the use of ‘true copies’ which was removed from the 2015 version. |
| DELETION | The definition of lifecycle (section 6.6) has been revised in 2018 and omits the previously specified duration of archival arrangements and retrievability of data for inspection as the 2015 version did. |
| DELETION | The concept of a ‘primary record’ from the 2015 version has been removed from the current version. This removes confusion and perhaps bad practices that the 2015 version may have appeared to support. |
| ADDITION | The revised definition of “Raw Data” in section 6.2 now includes ‘source data’ as defined in ICH GCP guidance. It also provides additional detail on simple electronic instruments such as pH meters or balances that may or may not store electronic data. Guidance is provided on how firms should manage the situations where electronic data are retained. |
| ADDITION | Section 6.5 on ‘data governance’ now includes requirements to ensure this is included in Quality Agreements, and that data are ‘directly accessible on request from national competent authorities.’ |
| ADDITION | Section 6.7 on ‘Recording and Collection of Data’ is new in the 2018 version. |
| ADDITION | Section 6.8 on data transfer / migration is new in the 2018 version. Data transfer processes should be validated. This section also addresses the requirements for use of “electronic worksheets” which I interpret to be spreadsheets such as Excel® |
ADDITION Section 6.9 on “Data Processing” is new in the 2018 version and requires traceability of “user defined parameters” and addresses expectations for activities such as re-integration of chromatography data to ensure it is not being ‘manipulated to achieve a more desirable result.’

ADDITION The 2018 revision adds section 6.10 on ‘Excluding Data’ that is not included in the 2015 version. For data that are excluded, the justification for doing so should be documented and all data should be retained and available for review. This section does not apply to GPvP where this is covered by pharmacovigilance legislation.

ADDITION The 2018 version adds section 6.14 addressing electronic signatures; this is totally new, and the section is expanded from the version in the draft guidance. They reference the MHRA / HRA Draft Guidance on the use of electronic informed consent for the GCP area.

ADDITION Section 6.20 on IT Suppliers and Service Providers is added to the 2018 guidance version. This is an important and welcome addition and addresses software as a service, platforms as a service and infrastructure as a service.

ADDITION The glossary adds new terms and their definition including: eCRF, ECG, Data Quality, DIRA, Data Cleaning, Directly Accessible, Advanced Electronic Signatures.

REVISION The definition of “Data” (section 6.1) has been revised to be more detailed than simply noting it is “information derived or obtained from raw data” and to include the “+” attributes of “ALCOA +” though it does not use this term. Data are to be Complete, Consistent, Enduring and Available in addition to meeting the ALCOA attributes.

REVISION The revised definition of ‘data integrity’ (section 6.4) now includes the requirement to incorporate risk management; “…quality and risk management systems including adherence to sound scientific principles and good documentation practices.” The definition is also substantially expanded from the one sentence version in the 2016 draft guidance.

REVISION The section on original record / true copy in the 2015 version is now divided into two sections (6.11.1 titled Original Record and 6.11.2 titled True Copy).

**ORIGINAL RECORD:** This section is revised to address GCP examples such as medical imaging results. It also is expanded to include examples where manual observations such as manual titrations or visual interpretations may need to be supported by second person verification.

**TRUE COPY:** This section has been revised to state that true copies may be stored in a different electronic format file to the original under specific circumstances. This section also states that when relying on ‘true copies’ the firm should consider the risks that may be associated with the destruction of the original records. It also provides specific information on
what should be verified to ensure a ‘true copy’ includes adequate content. The new version also addresses how to accommodate the situation here computer systems are no longer supported.

**REVISION**

The section on “Computerised System Transactions” (section 6.12) now addresses that the time interval before saving of data should be minimized for the situations where multiple operations are combined into a single transaction. A paragraph is now included in the 2018 version that addresses factors in this area that should be considered during system design.

The two figures in the 2015 version are not included in the 2018 document. For those of us who aren’t IT experts, the figures provided added value.

**REVISION and DELETION**

The definition of *audit trail* has been substantially expanded in section 6.13 of the 2018 version. Further, some of the explanation provided in the 2018 version is expanded and states that when the system administrator amends or turns off the audit trail that action should be recorded and retained.

The 2015 version states that systems should have *audit trails and unique login capability by the end of 2017*. The 2018 version removes a specific date for meeting this requirement but does not remove the requirement.

**The 2018 version states:** “Where relevant audit trail functionality does not exist (e.g. within legacy systems) an alternative control may be achieved for example defining the process in an SOP and use of log books. Alternative controls should be proven effective.

Where add-on software or a compliant system does not currently exist, continued use of the legacy system may be justified by documented evidence that a compliant solution is being sought and that mitigation measures temporarily support the continued use.”

1 It is expected that GMP facilities with industrial automation and control equipment / systems such as programmable logic controllers should be able to demonstrate working towards system upgrades with individual login and audit trails (reference: Article 23 of Directive 2001/83/EC)”

The 2018 version addresses audit trail review and states that these may be reviewed as a list of relevant data or by an ‘exception reporting’ process. This guidance defines the content of an exception report and states it is a ‘validated search tool.’ Further, reviewers must have ‘sufficient knowledge and system access to review relevant audit trails, raw data and meta data.’

MHRA also states they may identify a deficiency when systems that do not meet audit trail or individual user account expectations do not have remediation identified or subsequently implemented.
**REVISION**

Data Review and Approval, described in section 6.15 is expanded over the previous version. The revision also states that "Data review should be documented and the record should include a positive statement regarding whether issues were found or not, the date that review was performed and the signature of the reviewer." As part of gap assessments, firms should consider how they address the requirement for a ‘positive statement’ regarding the data review.

This section also addresses features of data review when a different organization generated the data, e.g., contract laboratories or contract manufacturers. In my opinion, this is an important addition.

**REVISION**

Section 6.16 addresses computerized system **user access/system administrator roles** is revised to 1) address login at the operating system and the application levels 2) addresses MRP systems that may have non-GXP components, and 3) revision of access rights depending on clinical trial status for GCP documentation.

**REVISION**

Section 6.17 on **Data Retention** adds the term ‘validated’ to describe the scanning process for paper records. The 2018 version does not address the circumstances where data are retained by a third party.

**REVISION**

Sections 6.17.1 and 6.17.2 on **archive and backup** respectively have been substantially expanded. The archive section specifically addresses how to manage legacy systems.

**REVISION**

Section 6.18 on **file structure** has been simplified and shortened. Details of flat files vs relational database structure has been eliminated.

**CONCLUSION:**

The additional detail and new topics identified in this guidance is welcome. The expanded detail covers important areas for which little guidance is currently available, for example the area of IT suppliers and service providers. The use of software as a service, platforms as a service and infrastructure as a service continues to increase in the industry. For firms that perform gap assessments against guidance documents, particularly data integrity guidance, they would be well served by repeating that assessment with this revision of the MHRA guidance. Many sections that were not addressed in the 2015 guidance have been added in this revision and many others have been significantly expanded in the level of detail. It does not appear that new, unexpected requirements are identified in this update, but the level of detail in explanations and examples certainly provide additional clarity and may result in a shift in firms’ interpretations. We will continue to follow this to determine if any changes in enforcement are reported as a result.

[BACK TO MAIN BLOG PAGE](#)