Recent Regulatory Guidance on Data Integrity

Lorrie D. Divers, President
QRCP Solutions, Inc.

27 March 2019: UR SCORE
Study Coordinators Organization for Research & Education
OBJECTIVES

► Refresher on principles of GCP data integrity and risk based management
► Review recent US and EU regulatory guidance on data integrity
► Understand how these non-GCP guidance documents can help ensure GCP compliance and data integrity
What is GCP Concerned With?

- Protection of rights, safety and welfare of human subjects
- Control of test article
- Data integrity
What is It?

data
/ˈdaːtə, ˈdætə/
noun

integrity
/inˈtegrəti/
Duke Whistleblower Gets More Than $33 Million In Research Fraud Settlement

March 25, 2019 - 5:03 PM ET

BILL CHAPPELL
Duke University is paying the U.S. $112.5 million to resolve allegations that it violated the False Claims Act by submitting falsified research data to win or keep federal grants. Here, a photo shows the Duke University Hospital in Durham, N.C., in 2008, when some of the fraud was alleged to have taken place.

Chris Keane/Reuters

Duke University is paying the U.S. government $112.5 million to settle accusations that it submitted bogus data to win federal research grants. The settlement will also bring a $33.75 million payment to Joseph Thomas, the whistleblower who drew attention to the fraud when he worked for Duke.

Thomas, a former Duke lab analyst, sued the university on behalf of the federal government, saying that a Duke researcher fudged data to help the university win and keep lucrative grants from two agencies, the National Institutes of Health and the Environmental Protection Agency.

$146.25 million
Data Integrity in Clinical Research

- Valid scientific design
- **Accurate** and **timely** data collection
- **Complete** and accurate report of results
- Ability to **reproduce** the results
  - Reconstruct the conduct of the clinical trial
Why Does Data Integrity Matter?

Accurate, complete, reliable data protects and respects subjects’ rights, safety and welfare.

For example, whether to end the study early because the treatment does not appear to be effective or is causing severe side effects.
Why Does Data Integrity Matter?

Inaccurate or incomplete (or falsified) data negatively impacts current study subjects care and rights

And potentially future patients if the product is approved for marketing based on that inaccurate data
Who is Responsible for Data Integrity?

Maintaining data integrity throughout the entire clinical development process is both a regulatory (legal) requirement and an ethical obligation for everyone involved.

- Sponsor, CRO, Study Sites, IRBs
- Principal and Co-Investigators, Study Coordinators, Pharmacist, Other Personnel
And now a word about...
During the past two decades, the number and complexity of clinical trials have grown dramatically. At the same time, increasing use of electronic systems and records and improvements in statistical assessments, present opportunities for alternative monitoring approaches (e.g., centralized monitoring) that can improve the quality and efficiency of sponsor oversight of clinical investigations. FDA encourages sponsors to develop monitoring plans that manage important risks to human subjects and data quality and address the challenges of oversight in part by taking advantage of the innovations in modern clinical trials. A risk-based approach to monitoring does not suggest any less vigilance in oversight of clinical investigations. Rather, it focuses sponsor oversight activities on preventing or mitigating important and likely risks to data quality and to processes critical to human subject protection and trial integrity. Moreover, a risk-based approach is dynamic, more readily facilitating continual improvement in trial conduct and oversight. For example, monitoring findings should be evaluated to determine whether additional actions (e.g., training of clinical investigator and site staff, clarification of protocol requirements) are necessary to ensure human subject protection and data quality across sites.

*Guidance for Industry Oversight of Clinical Investigations — A Risk-Based Approach to Monitoring, FDA, August 2013*
Sponsors **should focus on trial activities essential to ensuring human subject protection and the reliability of trial results**. Quality management includes the design of efficient clinical trial protocols and tools and procedures for data collection and processing, as well as the collection of information that is essential to decision making.

The **methods used to assure and control the quality of the trial should be proportionate to the risks inherent in the trial and the importance of the information collected**. The sponsor should ensure that all aspects of the trial are operationally feasible and should avoid unnecessary complexity, procedures, and data collection. Protocols, case report forms, and other operational documents should be clear, concise, and consistent.

**The quality management system should use a risk-based approach as described below.**

*INTEGRATED ADDENDUM TO ICH E6(R1): GUIDELINE FOR GOOD CLINICAL PRACTICE E6(R2), November 2016 (ICH); March 2018 (FDA)*
ICH E6(R2): Sections 5.0.1 - 5.0.7

5.0.1 Critical Process and Data Identification
During protocol development, the sponsor should **identify those processes and data that are critical to ensure human subject protection and the reliability of trial results**.

5.0.2 Risk Identification
The sponsor should identify risks to critical trial processes and data. **Risks should be considered at both the system level (e.g., standard operating procedures, computerized systems, personnel) and clinical trial level (e.g., trial design, data collection, informed consent process)**.

5.0.3 Risk Evaluation
The sponsor should evaluate the identified risks, against existing risk controls by considering:
(a) The **likelihood** of errors occurring.
(b) The extent to which such errors would be **detectable**.
(c) The **impact** of such errors on human subject protection and reliability of trial results.

[other sections include Controls, Communication, Review, and Reporting]
But This Doesn’t Apply to Me....
But This Doesn’t Apply to Me....

- Regulations are minimum requirements
- ICH guidance is FDA guidance and does not conflict with US Federal regulations
  - Helpful guidance to support compliance
- Provides greater protection for research subjects rights, safety and welfare
  - Strengthens data integrity
Recent Guidance on Data Integrity

- Medicines & Healthcare products Regulatory Agency (MHRA) ‘GXP’ Data Integrity Guidance and Definitions, March 2018

- Data Integrity and Compliance With Drug CGMP, Questions and Answers, Guidance for Industry, December 2018
Recent Guidance on Data Integrity

- Regulatory Education for Industry (REdI): FDA & MHRA Good Clinical Practice Workshop: Data Integrity in Global Clinical Trials - Are We There Yet? October 23-24, 2018
  - *Link to presentations provided on Reference slide*
  - Particularly recommend those by Fisher, Francis, Mulinde, Vinter and a joint FDA-MHRA presentation by Francis - Mulinde
Recent Guidance on Risk Based Approach

- Reflection paper on risk based quality management in clinical trials, EMA/269011/2013, 18 November 2013

But This Doesn’t Apply to Me....

- Guidance documents represent regulatory agencies ‘thinking’ on critical compliance topics of general applicability.

- Can provide direction and/or practical advice on GxP shared challenges that can be useful for clinical trials.
  - ‘X’ includes ‘C’ (as in GCP...)

Copyright, QRCP Solutions, Inc.
1. Background: “The way regulatory data is generated has continued to evolve in line with the ongoing development of supporting technologies such as the increasing use of electronic data capture, automation of systems and use of remote technologies; and the increased complexity of supply chains and ways of working, for example, via third party service providers. Systems to support these ways of working can range from manual processes with paper records to the use of fully computerised systems. The main purpose of the regulatory requirements remains the same, i.e. having confidence in the quality and the integrity of the data generated (to ensure patient safety and quality of products) and being able to reconstruct activities."
2. Introduction, 2.6: “This guidance aims to promote a **risk-based approach** to data management that includes data risk, criticality and lifecycle. Users of this guidance need to **understand their data processes** (as a lifecycle) to identify data with the greatest GXP impact. From that, the **identification of the most effective and efficient risk-based control** and review of the data can be determined and implemented.”
‘Understanding Data Processes’: A Case Study

NTF in multiple study subjects chart stated, "Study drug administration times were recorded in error."

- Study medication had to be administered after a bacterial swab was taken
- Study medication was visibly different than placebo so could not be administered by PI
- Not resolved by the Monitor during the study
‘Understanding Data Processes’: A Case Study

- Nearly half of the subjects had to be excluded from per protocol treatment analysis for this data discrepancy
- Five minutes discussing with the PI......
3. The principles of data integrity

“3.1 The organisation needs to take responsibility for the systems used and the data they generate. The organisational culture should ensure data is complete, consistent and accurate in all its forms, i.e. paper and electronic.

ALCOA + CCEA
ALCOA + CCEA

- Attributable
- Legible
- Contemporaneous
- Original
- Accurate
- Complete
- Consistent
- Enduring
- Available
3.2 Arrangements within an organisation with respect to people, systems and facilities should be designed, operated and, where appropriate, adapted to support a suitable working environment, i.e. creating the right environment to enable data integrity controls to be effective. “
MHRA ‘GXP’ Data Integrity Guidance

“3.3 The impact of organisational culture, the behaviour driven by performance indicators, objectives and senior management behaviour on the success of data governance measures should not be underestimated.”
MHRA ‘GXP’ Data Integrity Guidance

“3.6 The effort and resource applied to assure the integrity of the data should be commensurate with the risk and impact of a data integrity failure to the patient or environment. Collectively these arrangements fulfil the concept of data governance.

3.7 Organisations should be aware that reverting from automated or computerised systems to paper-based manual systems or vice-versa will not in itself remove the need for appropriate data integrity controls.”
MHRA ‘GXP’ Data Integrity Guidance

4. Establishing data criticality and inherent integrity risk

“4.1 Data has varying importance to quality, safety and efficacy decisions. Data criticality may be determined by considering how the data is used to influence the decisions made.

In reference to risks and controls
MHRA ‘GXP’ Data Integrity Guidance

4.2 The risks to data are determined by the potential to be deleted, amended or excluded without authorisation and the opportunity for detection of those activities and events. The risks to data may be increased by complex, inconsistent processes with open-ended and subjective outcomes, compared to simple tasks that are undertaken consistently, are well defined and have a clear objective.”
“4.3 Data may be generated by:

- (i) Recording on paper, a paper-based record of a manual observation or of an activity or
- (ii) electronically, using equipment that range from simple machines through to complex highly configurable computerised systems or
- (iii) by using a hybrid system where both paper-based and electronic records constitute the original record or
- (iv) by other means such as photography, imagery, chromatography plates, etc.”
4.5 The data integrity risk assessment (or equivalent) should consider factors required to follow a process or perform a function. It is expected to consider not only a computerised system but also the supporting people, guidance, training and quality systems. Therefore, automation or the use of a ‘validated system’ (e.g. e-CRF; analytical equipment) may lower but not eliminate data integrity risk. Where there is human intervention, particularly influencing how or what data is recorded, reported or retained, an increased risk may exist from poor organisational controls or data verification due to an overreliance on the system's validated state.”
MHRA ‘GXP’ Data Integrity Guidance

5. Designing systems and processes to assure data integrity; creating the ‘right environment’

Because we are all human... 5.1 provides a detailed list of considerations for designing systems and processes to facilitate compliance with the principles of data integrity

**Guess what the first point in that list is?**
MHRA ‘GXP’ Data Integrity Guidance

“• At the point of use, having access to appropriately controlled/synchronised clocks for recording timed events to ensure reconstruction and traceability, knowing and specifying the time zone where this data is used across multiple sites.”
Some other key considerations include:

- "Accessibility of records at locations where activities take place so that informal data recording and later transcription to official records does not occur.

- User access rights that prevent (or audit trail, if prevention is not possible) unauthorised data amendments. Use of external devices or system interfacing methods that eliminate manual data entries and human interaction with the computerised system, such as barcode scanners, ID card readers, or printers.

- The provision of a work environment (such as adequate space, sufficient time for tasks, and properly functioning equipment) that permit performance of tasks and recording of data as required.

- Access to original records for staff performing data review activities."
MHRA ‘GXP’ Data Integrity Guidance

6. Definition of terms and interpretation of requirements

- Provides terms and definitions, but also practical explanations of what they mean
- See for example 6.13, Audit Trail and 6.14 eSignatures
6.20. IT Suppliers and Service Providers (including Cloud providers and virtual service/platforms (also referred to as software as a service SaaS/platform as a service (PaaS) / infrastructure as a service (IaaS)).

“Where ‘cloud’ or ‘virtual’ services are used, attention should be paid to understanding the service provided, ownership, retrieval, retention and security of data.

The physical location where the data is held, including the impact of any laws applicable to that geographic location, should be considered.

The responsibilities of the contract giver and acceptor should be defined in a technical agreement or contract. This should ensure timely access to data (including metadata and audit trails) to the data owner and national competent authorities upon request. Contracts with providers should define responsibilities for archiving and continued readability of the data throughout the retention period (see archive).

Appropriate arrangements must exist for the restoration of the software/system as per its original validated state, including validation and change control information to permit this restoration.”
6.4 Data Integrity

“Data integrity is the degree to which data are complete, consistent, accurate, trustworthy, reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate. **Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices.**”
While this guidance is specifically for compliance with good manufacturing practices, it does have some useful ideas to consider for GCP data integrity

- Background section
- Questions 4 and 5 in particular
- Others need a bit more extrapolation....
FDA CGMP Data Integrity Compliance

“When considering how to meet many of these regulatory requirements, it may be useful to ask the following questions:

- Are controls in place to ensure that data is complete?
- Are activities documented at the time of performance?
- Are activities attributable to a specific individual?
- Can only authorized individuals make changes to records?
- Is there a record of changes to data?
- Are records reviewed for accuracy, completeness, and compliance with established standards?
- Are data maintained securely from data creation through disposition after the record’s retention period?”
“4. How should access to CGMP computer systems be restricted?

- The system administrator role, including any rights to alter files and settings, should be assigned to personnel independent from those responsible for the record content. To assist in controlling access, it is important that manufacturers establish and implement a method for documenting authorized personnel’s access privileges for each CGMP computer system in use (e.g., by maintaining a list of authorized individuals)....”
“5. Why is FDA concerned with the use of shared login accounts for computer systems?

- When login credentials are shared, a unique individual cannot be identified through the login and the system would not conform to the CGMP requirements in parts 211 and 212 [nor would it comply with GCP or Part 11 requirements]....”
FDA CGMP Data Integrity Compliance

“18. How does FDA recommend data integrity problems be addressed?

FDA encourages you to **demonstrate that you have effectively remediated your problems by investigating** to determine the problem’s scope and root causes, **conducting a scientifically sound risk assessment of its potential effects** (including impact on data used to support submissions to FDA), and **implementing a management strategy**, including a global corrective action plan that addresses the root causes. This may include retaining a third-party auditor and removing individuals responsible for data integrity lapses from positions where they can influence CGMP-related or drug application data at your firm. It also may include improvements in quality oversight, enhanced computer systems, and creation of mechanisms to prevent recurrences and address data integrity breaches (e.g., anonymous reporting system, data governance officials and guidelines).
In other words, ignoring the problem will NOT make it go away.....
What to Do?

- Understand your systems and processes for collecting, recording, reviewing, reporting and archiving data
  - Ask questions, don’t make assumptions
  - Especially for new or novel data or systems

- Evaluate risks
  - Systems and processes
  - Study specific

- Apply appropriate controls, including ‘real time’ actions and independent reviews
  - “An ounce of prevention is worth a pound of cure.” [B.Franklin]
  - Example: Scanning documents
What to Do?

- Review / Monitor / Audit from the perspective of *data integrity*
  - Review data *across* subjects
  - Data logic - *Does this make sense clinically?*
  - Late entries / Entries made on the same date
  - Repetitive errors
  - Excessive / Improper corrections
  - Inappropriate personnel completing records
What to Do?

- Validate all computer/software systems that capture, record, store and/or report data
  - Laboratory instrument interface software (‘middleware’) is data related software
  - ‘Trust but verify’
    - Is it really functioning as expected/required for the study?
    - Data entry errors can still occur
What to Do?

- Know what is in audit trails **before** an issue occurs
  - Contains adequate information to verify data integrity in a logical format and **is not editable**

- Control access to systems, data and records
  - **DO NOT SHARE LOGINs and/or PASSWORDs**
  - Do not walk away from an active program
  - Do not leave source documents lying about....
What to Do?

Consider human nature

- We all make mistakes *but* are people amenable to correcting them and learning (not repeating them)?

- How can a process be designed, or a system controlled, in ways that support data integrity (and help us error prone humans)?
  - A simple example is ‘smart’ form design
What to Do?

Everyone involved in clinical trials must always act in ways that protect and respect study subjects’ rights, safety and welfare and ensure data integrity.
Questions?

Visit our website: www.qrcpsolutions.com
➢ Follow us on LinkedIn!

Contact us at: ldivers@qrcpsolutions.com
References and Further Reading

- Regulatory Education for Industry (REdI): FDA & MHRA Good Clinical Practice Workshop: Data Integrity in Global Clinical Trials - Are We There Yet? October 23-24, 2018

- Medicines & Healthcare products Regulatory Agency (MHRA) ‘GXP’ Data Integrity Guidance and Definitions, March 2018
References and Further Reading

- Reflection paper on risk based quality management in clinical trials, EMA/269011/2013, 18 November 2013

- US Dept. of HHS, Office of Research Integrity, Handling Misconduct (main page)
  https://ori.hhs.gov/handling-misconduct
References and Further Reading

- ICH E6(R2) and Data Integrity: Four Key Principles Clinical Researcher, April 17, 2018 Clinical Researcher—April 2018 (Volume 32, Number 4) ICH IN FOCUS, Michael Rutherford, MS, [DOI: 10.14524/CR-18-4021]
  https://acrpnet.org/2018/04/17/ich-e6r2-data-integrity-four-key-principles/

- What is Data Integrity and ALCOA Plus, Pharma Awareness, 21/01/2019 (graphic on slide 26)