BIENVENIDO WELCOME BIENVENUE WILLKOMMEN

OMNICOMM INNOVATION FORUM EUROPE 2017

BENVENUTI VELKOMMEN WELKOM ברוכים הבאים

OmniComm®

20 Years of EDC Specialization & Integration

Data Integrity – Why is it important?

24 March 2017

Maibritt Haugaard Møller, System Validation Expert
Mette Ravn, Vice President, Data Management, IT and System Validation

Overview of the Content of the presentation

- Short introduction to Larix, a Nordic Full Service CRO
- Brief history of Data Integrity & issues
- Principles of Data Integrity ALCOA+
- Data Integrity Governance
- Data Integrity Life Cycle
- IT Support for Data Integrity
- Assessing a system for Data Integrity (examples)
- Regulatory References, Guidance & Requirements
- Wrap up
- Questions

Short Introduction to Larix

Larix a Nordic Full Service CRO - history

- Established in 2001 as an independent consultant
- From 2003 CRO services within Data Management and Statistics
- From 2008 services within Clinical Research and independent QA function
- From 2010 full service CRO incl. Pharmacovigilance
- From February 2015 Larix operates a Swedish subsidiary in Stockholm
- From July 2015 Larix takes over NORMAs activities in Norway, Sweden, Finland and Denmark
- Today Larix A/S is the largest CRO in Scandinavia within Biometrics
- Employees +70 heads
- Customers mainly from Medicon Valley and Europe
- Financially robust
  - Gazelle Awards 2011-2012-2013

Larix – provides today

A full range of services to the pharmaceutical, biotech, medical device and function food industry within:

- Clinical Operations
- Pharmacovigilance
- Medical Monitoring
- Data Management
- Statistics/Programming
- Science & Medical Writing
- GCP and Vendor Audits
- System Validation
- DMC

Notification

- Disclaimer:
  - *Information presented in this document reflects the current opinion of the authors at the publication date about the concerned subjects. This document is provided for documentation only*
  - *Contained information may be subject to change*

Brief history of Data Integrity

Brief history of Data Integrity & issues

Data Integrity is not new:

Data Integrity in all GXP regulated disciplines is the current hot topic with regulatory agencies and is either due to falsification of data or poor management leadership, poor data management practices and poor training, specifically for Data Integrity. And it is a global issue. Already described decades ago in e.g.:

- UK Orange Guide in 1971
- EU GMP Chapter 4 (early 1980s)
- EU GMP Annex 11 (early 1980s)
- EU Annex 11 in 1992
- …….

The regulatory authorities want to increase and ensure control, quality and data integrity to avoid falsifications.

Brief history of Data Integrity issues cont...

Examples of data integrity issues:

Two data integrity issues from the early 1990s:

- Barr Laboratories. It was found that the laboratory was re-testing and re-sampling until the batch passed. This case ended in court.
- Able Laboratories fraud case was a major issue where manipulation or falsification of data to pass, was found in 2005

One example from 2016

More than four out of five Chinese executives surveyed, reported their companies had fallen victim to fraud during the last 12 months

Principles of Data Integrity
ALCOA+

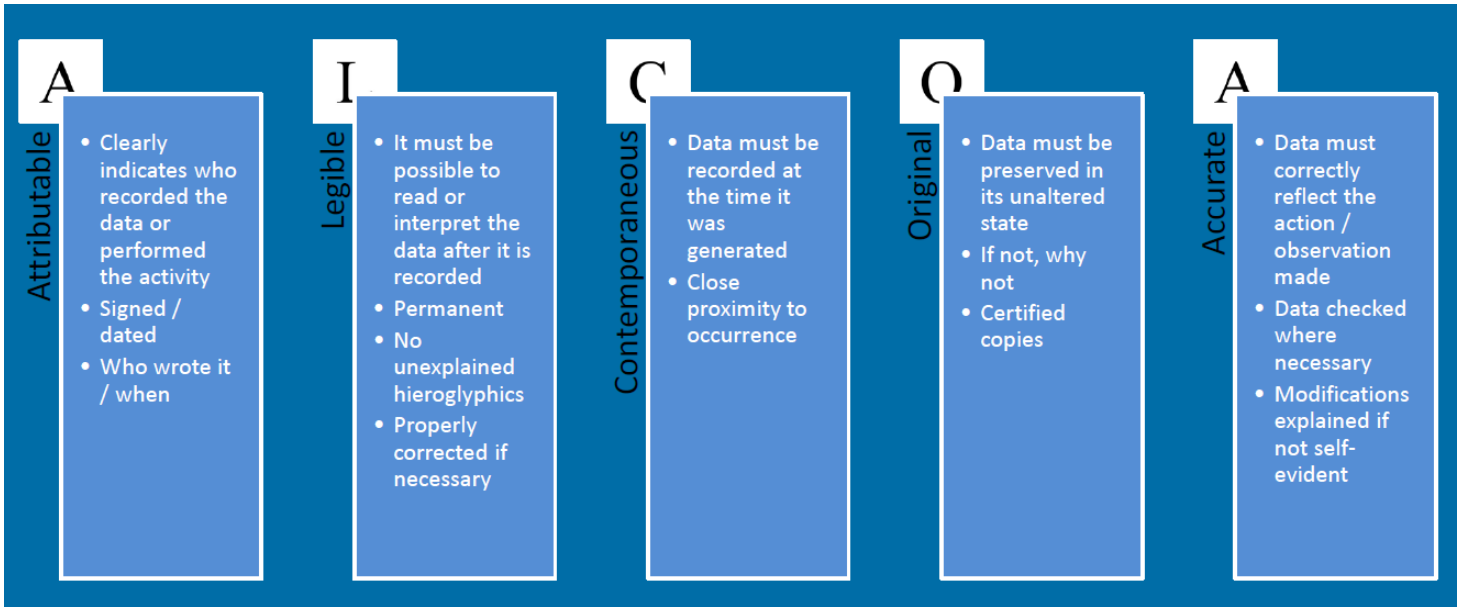
Definition of Data Integrity

Data Integrity:

Is the maintenance of, and the assurance of the accuracy and consistency of, **data** over its entire **life cycle**, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

ALCOA+ Principles

The first 5 principles are developed by FDA



- A commonly used acronym for ‘attributable, legible, contemporaneous, original and accurate’, which puts additional emphasis on the attributes of being complete, consistent, enduring and available – implicit basic ALCOA principles

ALCOA+ Principles cont...

The new 4 ALCOA+ principles are developed by EMA

Complete: All data must at all time be present and available, including any repeated sampling or re-analysis performed on the sample.

Consistent: All parts of a data set, such as the sequence of events must be dated and/or time-stamped in expected sequence.

Enduring: All data must be stored on proven storage media whether it is documented on paper/electronically.

Available: Over the lifetime of a data set it must be available for review, audits and inspections.

ALCOA+ Principles cont...

Data Integrity must be secured through the complete data life cycle (from data creation -> data deletion) and all involved systems e.g. (**TrialMaster vs. CTMS/eDiary systems**) are impacted by the Data Integrity requirements).

Data Integrity Governance

Data Integrity Governance

Data Integrity Governance:

Data governance is the sum total of arrangements which provide assurance of Data Integrity.

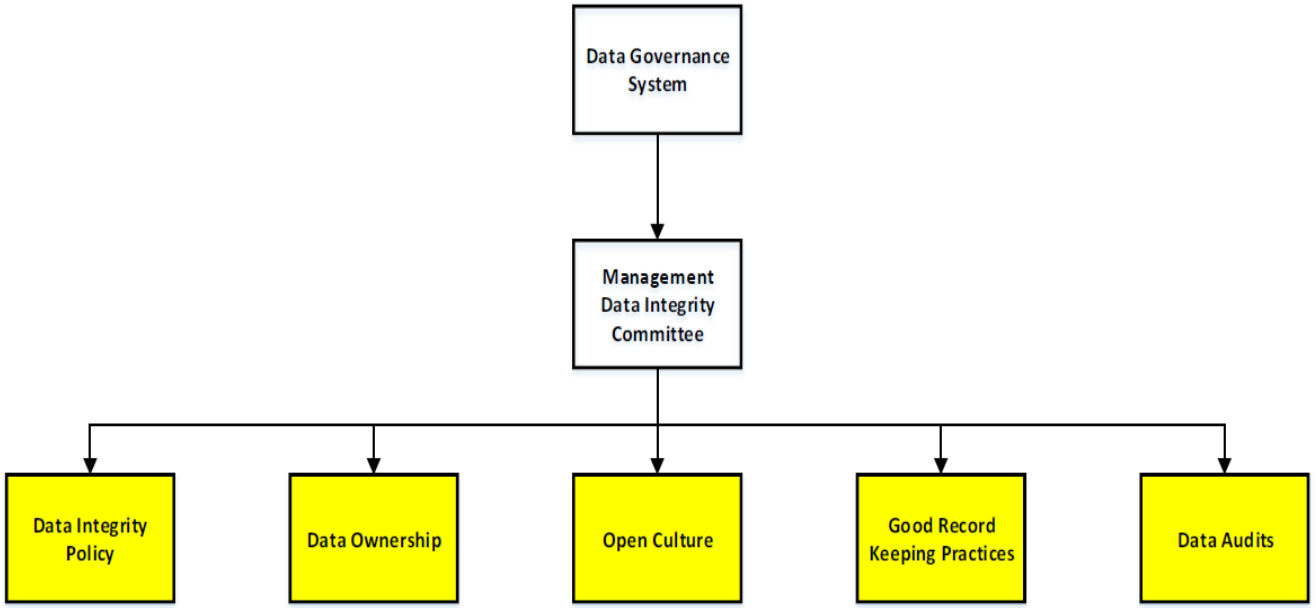
The principles of Data Integrity are not limited to compliance with regulatory requirements, but extend to the general state of awareness, mind set and culture of all staff regarding Data Integrity and prevention of issues. This can be achieved by establishing a data governance program within the QMS focusing on:

- Management Leadership
- Procedural (Policies) for data handling
- Behavioral (Culture): Introducing/teaching/practicing appropriate organizational behavior when handling data
- Technical (Process): Having appropriate processes for handling, recording, processing, archiving and decommissioning of data
- Assessment and remediation of existing processes and systems for generating, interpreting, reporting and storing data

Data Integrity Governance cont...

Data Integrity Governance System:

Senior Management must be engaged. Senior Manager under the EU GMP Chapter 1 and ICH Q10 is responsible for the overall quality system and that includes Data Integrity.



Data Integrity Governance cont...

Data Integrity Governance System: Data Management Governance:

A robust and sustainable good data management system requires data management governance, including:

- application of modern Quality Risk Management (QRM) principles and good data management principles that assure the validity, completeness and reliability of data;
- application of appropriate quality metrics;
- assurance that personnel are not subject to commercial, political, financial and other pressures or incentives that may adversely affect the quality and integrity of their work;
- allocation of adequate human and technical resources such that the workload, work hours and pressures on those responsible for data generation and record keeping do not increase errors;

Data Integrity Governance cont...

Data Integrity Governance System: Data Management Governance:

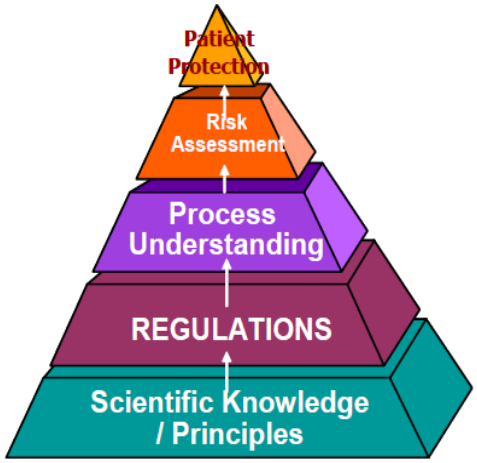
Core principles of Risk Management:

Core principles of risk management include the follow general tenants:

1. *Compliance with applicable laws is an absolute requirement* - Risk assessment is to be used to assess how to assure compliance and the resulting prioritization for action -- not for a decision regarding the need to fulfill applicable regulations or other legal requirements.

2. *Risk can only be effectively managed when it is identified, assessed, considered for further mitigation and communicated* - This principle embodies the four general stages to an effective quality risk management process as defined by ICH Q9: 1) Risk Assessment (to include risk identification, analysis, and evaluation, 2) Risk Control (to include risk reduction and acceptance), 3) Risk Communication, and 4) Risk Review.

Diagram 1: *Quality Risk Evaluation Pyramid*



Data Integrity Governance cont...

Data Integrity Governance System: Quality Culture:

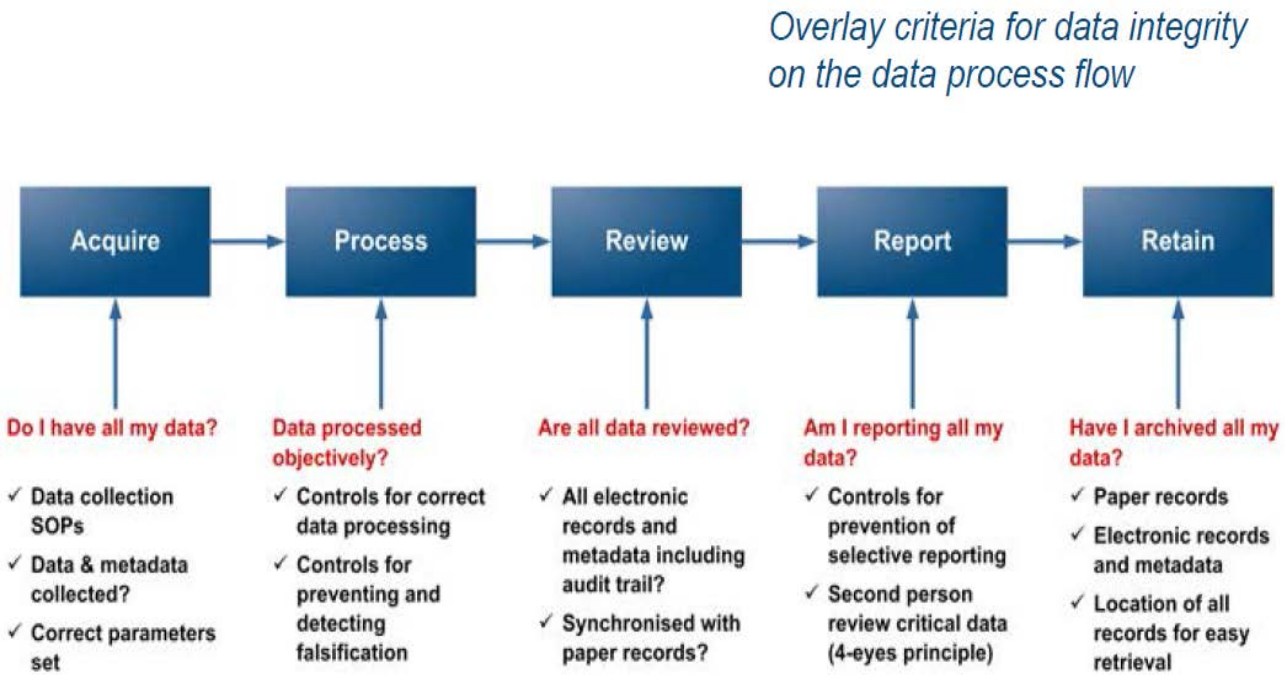
Maintain:

- A working environment that minimizes the risk of non-compliant records and erroneous records and data;
- Transparent and open reporting of deviations, errors, omissions and aberrant results at all levels of the organization;
- Steps should be taken to prevent, and to detect and correct weaknesses in systems and procedures that may lead to data errors so as to continually improve the robustness of scientific decision-making within the organization;

Data Integrity Governance cont...

Data Integrity Governance System: Data Management Governance:

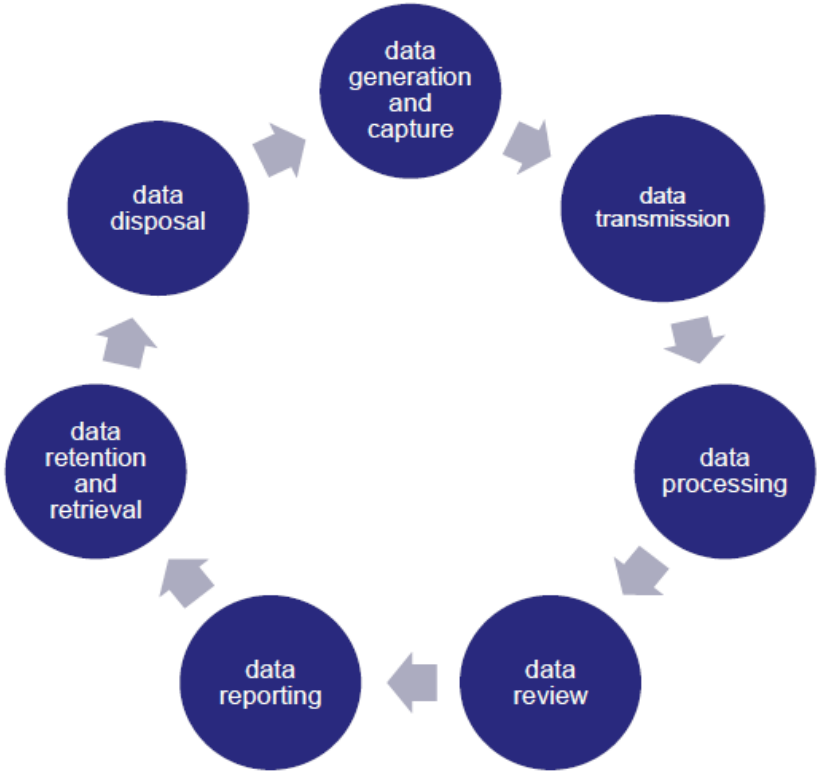
Data Integrity controls



Data Integrity Life Cycle

Data Integrity – Data Life Cycle

The Data Life Cycle refers to how data is generated, processed, reported, checked and used for decision-making, stored and finally discarded at the end of retention period.



Data Integrity – Data Life Cycle cont...

Validation should include assessing risk and developing quality risk mitigation strategies, including controls to prevent and detect risks throughout the Data Life Cycle.

- determining the risk-based approach to reviewing electronic data and audit trails based upon process understanding and knowledge of potential impact on products and patients;
- writing SOPs defining review of original electronic records and including meaningful metadata such as audit trails and review of any associated printouts or PDF records;

Data Integrity – Data Life Cycle cont...

Validation should include….

- documenting the system architecture and data flow, including the flow of electronic data and all associated metadata, from the point of creation through archival and retrieval;
- ensuring that the relationships between data and metadata are maintained intact throughout the Data Life Cycle.

IT Support for Data Integrity

IT Support for Data Integrity

The impact of IT infrastrucure on Data Integrity:

- IT facilities, environmental controls and physical security
- Qualified IT infrastructure and validated IT systems
- IT support
  - System management & administration
  - Back up & restore
  - Disaster recovery
- Change Management

IT Support for Data Integrity cont...

IT infrastructure Requirements:

- Qualified IT infrastructure
  - An IT infrastructure designed, implemented, operated and managed within a Quality Management System (QMS)

IT Support for Data Integrity cont…

IT infrastructure Requirements:

- IT infrastructure QMS should cover amongst others:
  - Configuration Management
  - Change Management
  - Security Management
  - Incident Management
  - Corrective and preventive action (CAPA)
  - Business continuity Management
  - Supplier/service provider Management
  - Periodic evaluation
  - Training Management
  - Etc……

Assessing a System for Data Integrity (examples)

Assessing a System for Data Integrity

Overall Approach: (internally in your organization)

- Analyze the proposed GXP systems and procedures
- Elaborate:
  - A list of assessing questions
  - A list of items to investigate
- Propose a concluding statement
  - Including recommendation

Assessing a System for Data Integrity cont...

Overall Approach: (externally)

Vendor Management: (depending on services provided)

- Frequently Audit your Suppliers/Service Providers
- Software for GXP systems: Ensure that the systems are validated. Is there documentation for validation of data integrity principles?
- Is the staff trained in GXP principles?
- Other…..

Assessing a System for Data Integrity cont...

Check the GXP Software - Audit Trails:

Annex 11 Volume 4: Clause 9 (Regulations for audit trail)

- Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all “GXP”/GMP -relevant changes and deletions (a system generated "audit trail").
- For change or deletion of “GXP”/GMP - relevant data the reason should be documented.
- Audit trails need to be available and convertible to a generally intelligible form (available for inspections) and regularly reviewed.

It is not described anywhere, what ”regularly” means; but it is something to consider and implement into your procedures (risk based approach).

Assessing a System for Data Integrity cont...

- Review of Audit Trail: TrialMaster (Data entered on Informed Consent Form):

Question	No.	Question Audit History				
		Response	Field Monitored?	Notes	Date/Time	Role
Date informed consent obtained:	1	- *Empty* -	False	- *Empty* -	20/JAN/2017 18:03:49 RT	Coordinator Site
		20/JAN/2017	False	- *Empty* -	20/JAN/2017 18:05:08 RT	Coordinator Site
		20/JAN/2017	False	Verify and correct the date of signature of the Consent is 19 / Jan / 2017	30/JAN/2017 16:16:52 RT	CRA/PM
		19/JAN/2017	False	Transcription Error	31/JAN/2017 21:35:05 RT	Coordinator Site
		19/JAN/2017	False	the data was corrected	31/JAN/2017 21:35:05 RT	Coordinator Site
		19/JAN/2017	False	Closed Query	14/FEB/2017 16:44:13 RT	CRA/PM
		19/JAN/2017	True	- *Empty* -	14/FEB/2017 16:44:26 RT	CRA/PM

Assessing a System for Data Integrity cont...

Regular review of Audit Trail – (regular?)

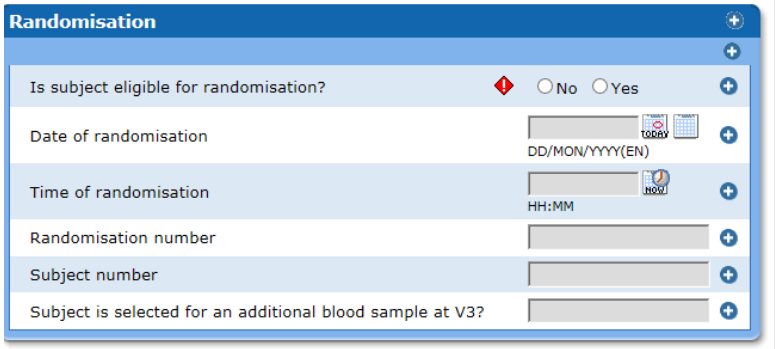
- Second person review (Risk based approach – critical data points): look at data generated by the system.

Documenting the review

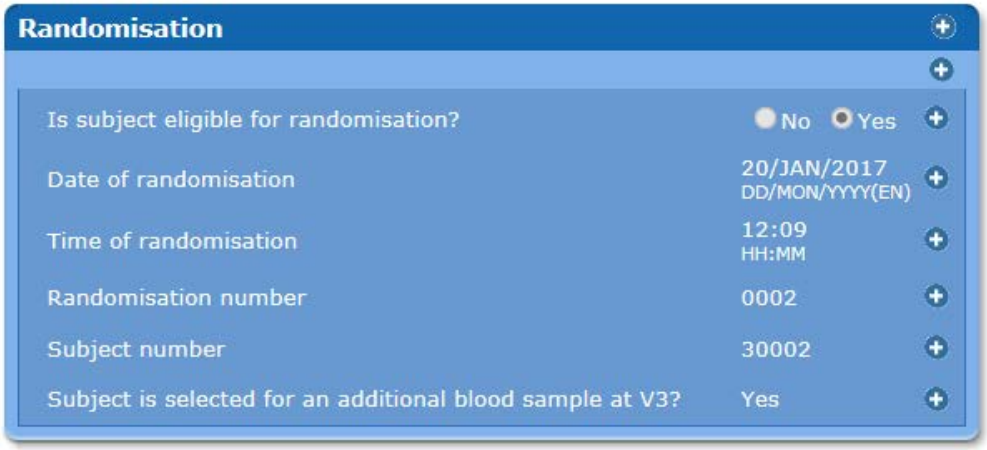
- Few systems (if any) have the ability to document if the audit trail has been reviewed, by whom and when.
- Future: we would like to have software functions in TrialMaster, supporting us with documentation of the review. E.g. a report that could show, when and by whom the review of the audit trail was performed.

Assessing a System for Data Integrity cont...

Using TrialMaster: (Randomization module/feature):



What if two subjects get the same randomisation number?



Assessing a System for Data Integrity cont...

What else can we do e.g. in our daily Data Management work?

UAT of study set up (A must)

- Design, Build, Test and properly document **(Good Documentation Practice)**

Range Check

- Build in range check to catch data entry errors or outliers

Edit Checks

- For e.g. data consistency, completenes, contemporaneous, availability etc.

Data Review

- Review and approval of critical data

Regulatory References, Guidance & Requirements

Regulatory References, Guidance & Requirements

ICH E6 (R2) Addendum

5.5 Trial Management, Data Handling, and Record Keeping

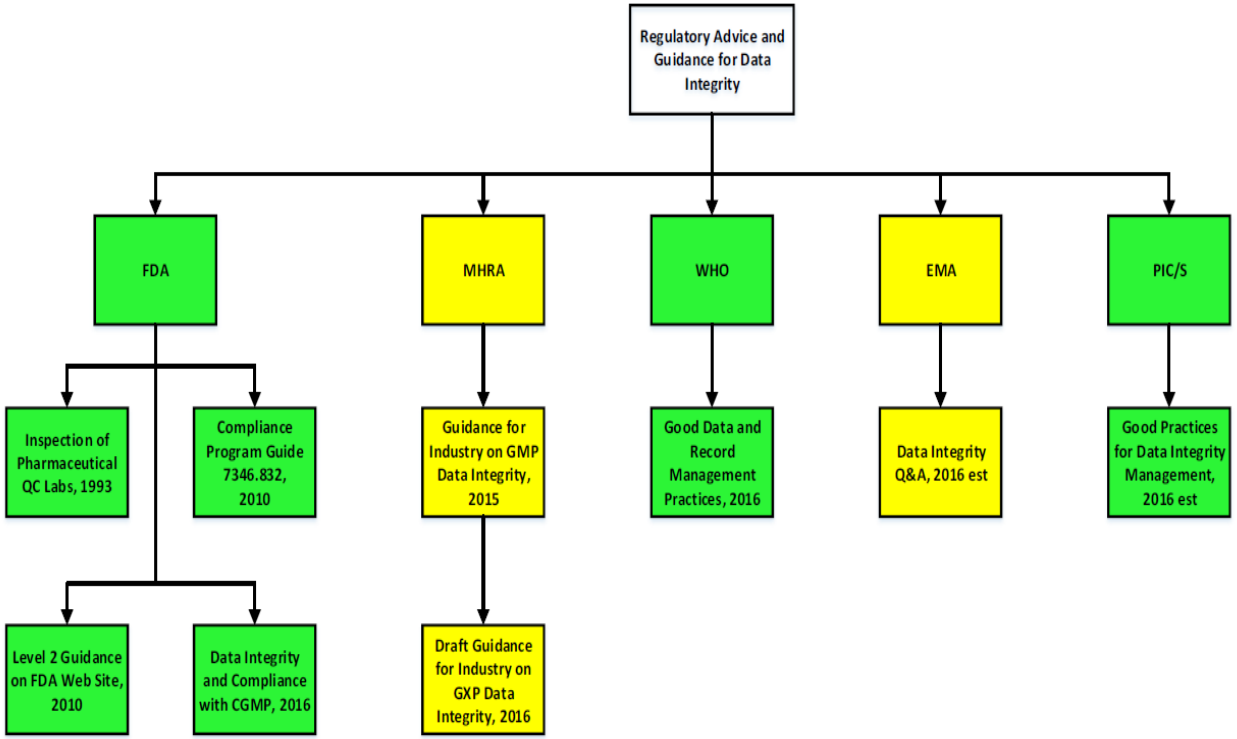
- **5.5.3** When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should: […]

ADDENDUM

- (h) *Ensure the integrity of the data including any data that describe the context, content and structure of the data. This is particularly important when making changes to the computerized systems, such as software upgrades or migration of data.*

Regulatory References, Guidance & Requirements cont...

Regulatory References, Guidance & Requirements which can help us ensuring Data Integrity:



Regulatory References, Guidance & Requirements cont...

Among others… Relevant documents to consider investigating further:

WHO Expert Committee on Specifications for Pharmaceutical Preparations, Annex 5 Guidance on good data and record management practices

http://www.who.int/medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf

EMA GMP/GDP Q&A, Data Integrity:

http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q_and_a/q_and_a_detail_000027.jsp

PIC/S draft guidance GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS

https://www.picscheme.org/useruploads/documents//PI_041_1_Draft_2_Guidance_on_Data_Integrity_2.pdf

Wrap Up

Wrap Up

Data Integrity is not new

Data Integrity in all GXP regulated disciplines is the current hot topic for regulatory agencies.

The expectations of the regulatory agencies are based on two basic rules:

- Burden of proof
  All claims are unproven until proven otherwise

- Legally sound
  The evidence supported through source data should be strong enough to make a case in the court.

Questions

Contacts:

- Maibritt Haugaard Møller, System Validation Expert, mha@larixcro.com
- Mette Ravn, Vice President, Data Management, IT & System Validation, mra@larixcro.com