Integrità del dato: ispezioni e deviazioni riscontrate

Dr. Luisa Stoppa

Life Science Data Congress 2017

Milano, 5 Luglio 2017

Agenzia Italiana del Farmaco
AIFA

Dichiarazione di trasparenza/interessi*

Le opinioni espresse in questa presentazione sono personali e non impegnano in alcun modo l'AIFA

Interessi nell'industria farmaceutica	NO	Attualmente	Da 0 a 3 anni precedenti	oltre 3 anni precedenti
INTERESSI DIRETTI:				
1.1 Impiego per una società: Ruolo esecutivo in una società farmaceutica	X	☐	☐	☐ obbligatorio
1.2 Impiego per una società: Ruolo guida nello sviluppo di un prodotto farmaceutico	X	☐	☐	☐ obbligatorio
1.3 Impiego per una società: altre attività	X	☐	☐	☐ facoltativo
2. Consulenza per una società	X	☐	☐	☐ facoltativo
3. Consulente strategico per una società	X	☐	☐	☐ facoltativo
4. Interessi finanziari	X	☐	☐	☐ facoltativo
5. Titolarità di un brevetto	X	☐	☐	☐ facoltativo
INTERESSI INDIRETTI:				
6. Sperimentatore principale	X	☐	☐	☐ facoltativo
7. Sperimentatore	X	☐	☐	☐ facoltativo
8. Sovvenzioni o altri fondi finanziari	X	☐	☐	☐ facoltativo
9. Interessi Familiari	X	☐	☐	☐ facoltativo

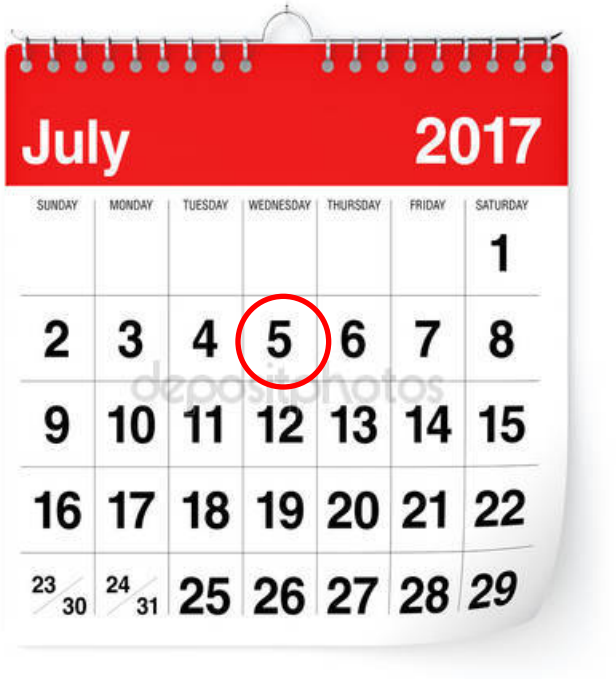
* Luisa Stoppa, secondo il regolamento sul Conflitto di Interessi approvato dal CdA AIFA in data 25.03.2015 e pubblicato sulla Gazzetta Ufficiale del 15.05.2015 in accordo con la policy EMA /626261/2014 sulla gestione del conflitto di interessi dei membri dei Comitati Scientifici e degli esperti.

N.B. Il compenso ricevuto per questo intervento è regolato dalla contrattazione collettiva.

Agenzia Italiana del Farmaco
AIFA

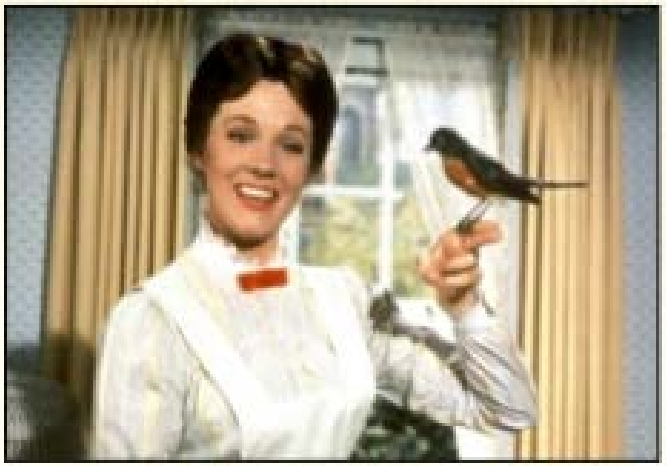
Agenda

- Data integrity
- Normative e linee-guida
- Data integrity / falsificazione
- Deviazioni ricorrenti
- Conclusioni



WHY? Data Integrity

Mary Poppins Style



In ev'ry job that must be done
There is an element of fun
you find the fun and snap,
The job's a game
and every task becomes a piece of cake

A spoonful of sugar helps the medicine go down
The medicine go down

WHY? Points of view

No data integrity
No data trace-back
No audit trail

Warning letter
Import alert
License withdrawal

Scandals
Bad publicity
Economic loss

Guidelines

EU-GMP Vol. 4 chapter 4: documentation (30 Giugno 2011)
EU-GMP Vol. 4 Annex 11: Computerised system (30 Giugno 2011)

FDA 21 CFR Part 11: e-records, e-signatures (Agosto 2003)
FDA Guidance for industry: Data Integrity and compliance with CGMP (Aprile 2016)

MHRA: GMP Data Integrity Definition & Guidance (Luglio 2016)

WHO: TRS 966 Guidance on Good Data and Record Management (2016, in revisione)

PIC/S: Good Practice for data management and integrity in regulated GMP/GDP enviroments (Agosto 2016, in revisione)

Guidelines

1992 — Annex 11 EU GMP

1997 — 21 CFR Part 11

2003 — Rev. 21 CFR Part 11

2011 — Rev. Annex 11 EU GMP
Rev. chapter 4 EU GMP

2015 — MHRA Guidance
WHO data management annex 5

2016 — FDA Guidance for industry
PIC/S draft 2 guideline
EMA Q&A data integrity
Rev. MHRA guidance
Rev. WHO annex 5

2017 — Rev. WHO (on going)
Rev. PIC/S guideline (on going)

Guidelines: WHO

Appendix 1: expectations and examples of special risk management considerations for the implementation of ALCOA 8-plus) principles in paper-based and electronic systems

Attributable	
Expectations for paper records	**Expectations for electronic records**
Attribution of actions in paper records should occur, as appropriate, through the use of: • initials; • full handwritten signature; • personal seal; • date and, when necessary, time.	Attribution of actions in electronic records should occur, as appropriate, through the use of: • unique user logons that link the user to actions that create, modify or delete data; • unique electronic signatures (can be either biometric or non-biometric); • an audit trail that should capture user identification (ID) and date and time stamps; • signatures, which must be securely and permanently linked to the record being signed.

Guidelines: PIC/S (revision)

Chapter 8: Expectations for the generation, distribution and control of records

Expectations	Potential risk of not meeting exp.
Documents should be stored in a manner which ensures appropriate version control. Master copy (in soft copy) should be prevented from unauthorised or inadvertent changes E.g.: For the template records stored electronically, the following precautions should be in place: -Access to master templates should be controlled - master documents should be stored in a manner which prevents unauthorised changes	Inappropriate storage conditions can allow unauthorised modification, use of expired and/or draft documents or cause the loss of master documents. The processes of implementation and the effective communication are just as important as the document. Master copies should contain distinctive marking so to distinguish the master from a copy, e.g. use of colored papers or inks so as to prevent inadvertent use

Guidelines: EU GMP Part I

Cap. 4 documentazione - Principle

Suitable controls should be implemented to ensure the accuracy, integrity, availability and legibility of documents. Instruction documents should be free from errors and available in writing. The term 'written' means recorded, or documented on media from which data may be rendered in a human readable form.

Punto 4.1

Appropriate controls for electronic documents such as templates, forms, and master documents should be implemented. Appropriate controls should be in place to ensure the integrity of the record throughout the retention period.

Punto 4.10

4.10 It should be clearly defined which record is related to each manufacturing activity and where this record is located. Secure controls must be in place to ensure the integrity of the record throughout the retention period and validated where appropriate.

Guidelines: EU GMP Part I

Annex 11 – Computerised system

1. ***Risk Management***

Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.

7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically.

17. ***Archiving***

Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

Guidelines

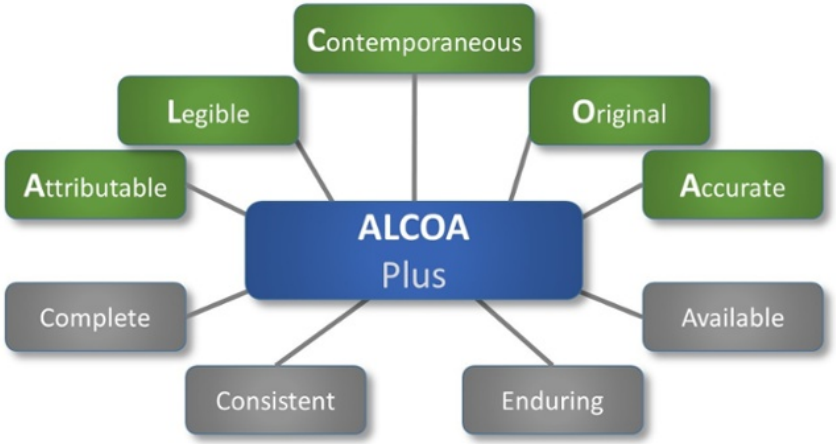
Definition: Data integrity is the degree to which a collection of data is complete, consistent and accurate throughou the data lifecycle.

The collected data should be Attributable, Legible, Contemporaneously recorded, Original or a true copy, and Accurate

ALCOA principles were developed for paper records (not sufficient for electronic records)
ALCOA +

Guidelines

Attributable: who acquired the data or performed an action and when?
Legible: can you read and understand the data entries?
Contemporaneously: documented at the time of activity
Original: first recorded observation
Accurate: no errors or editing without amendements



Guidelines

Complete: all data including any repeat or reanalysis performed

Consistent: all elements of the records such as the sequence of events, follow on and are dated or time stamped in expected sequence

Enduring: recorded in a permanent, maintainable form for the useful life

Available: for review and audit or inspection over the lifetime of the record

Guidelines

Data integrity is the degree to which a collection of data is complete, consistent and accurate throughou the data lifecycle

D.I. is equally applicable to both paper and electronic data

Is Data integrity a NEW regulatory expectations?

Data Integrity & Data Manipulation

There is a general misconception that data integrity failures only result from acts of deliberate fraud.

The majority of issues related to bad practice, poor organisational behaviour and weak systems, create opportunities for data to be manipulated.

Data Integrity		Data Manipulation
Preventing unintentional or unauthorised changes to data		Intentional changes to data

Frequent deviations

3 → 8

Frequent deviations

Not available

Available and not enabled

Available, enabled, not periodically verified

Available, enabled, periodically verified, not documented evidence of review

Not part of self inspection

Frequent deviations

Shared username and password for analytical software and the operating system

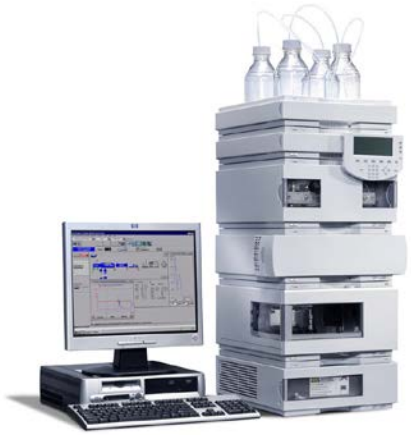
Shared generic ID [analyst]

Generic ID «Administrator» and pw «123456» shared by analyst to delete/overwrite data (.....space for more recent results)

pw available on the keyboard

Not automatic log-off

Frequent deviations



«Trial analysis»/ «Test standard» injections prior to beginning an official sequence of SST and analysis.....in case of deviations, it is not recorded and managed

HPLC processing methods (including integration parameters) not defined/not controlled

- manual integrations without justification or approval
- processing injections in the same sequence with different processing methods and integration parameters

Frequent deviations

Date and time stamps not locked

Uncontrolled templates used to record data / no reconciliation of issued blank forms

Logbook (complaints, deviations, OOS) as .xls / .doc files not locked

No documented on data review prior approval of analysis (metadata, audit trail, manual integration...)

Failure of periodical calibration of balance; calibrated again and original record not kept

Frequent deviations

Discrepancy between the number of incubated plates and the number described in SOP

Discrepancy between the number of points to be sampled and number of results (WFI, EM)

CFU under-estimated

microbiological tests opens the door to significant issues with data integrity

Conclusion

Short term actions:
- Gap analysis
- Risk analysis and action plan

Long term action:
- Training and communication, awareness of consequences
- Routine data verification
- Periodic surveillance (self inspection)

ANY POTENTIAL FOR COMPRIMISING THE RELIABILITY OF DATA IS A RISK