

dcvmn
Developing Countries Vaccine
Manufacturers Network

Regional workshop: Cost-effective Purification of Vaccines,
Data Integrity Systems and CTDs

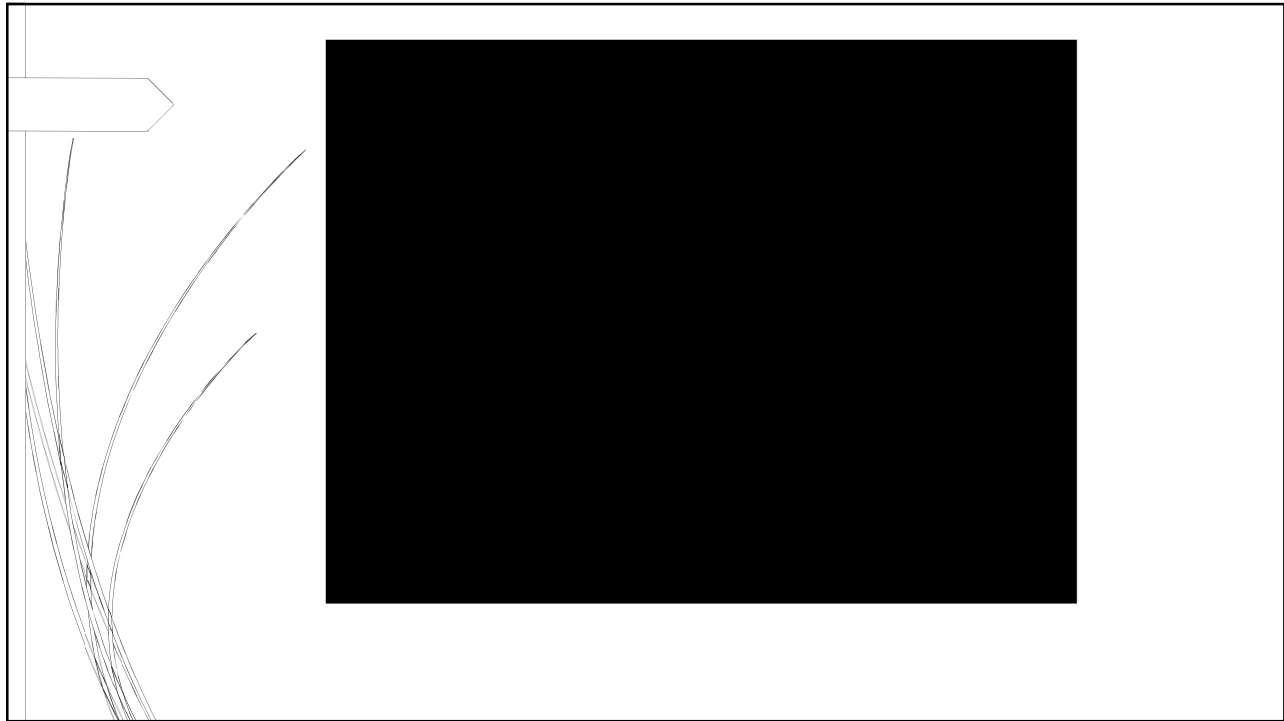
Dr. Sandra Olga Rumiano



dcvmn
Developing Countries Vaccine
Manufacturers Network

Data Integrity session
Hosted by DCVMN
Day 1

Dr. Sandra O. Rumiano
June 18th and 19th 2018



Some words to have in Mind

- Data: Facts, figures and statistics collected together for reference or analysis. All original records and true copies of original records, including source data and metadata and all subsequent transformations and reports of these data, that are generated or recorded at the time of the GXP activity and allow full and complete reconstruction and evaluation of the GXP activity.
- Metadata are data about data that provide the contextual information required to understand those data. These include structural and descriptive metadata. Such data describe the structure, data elements, interrelationships and other characteristics of data: 8 vs 8mg
- Revision and review
- Data integrity is the degree to which data are complete, consistent, accurate, trustworthy and 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, such that they are attributable, legible, contemporaneously recorded, original or a true copy and accurate.

- **Raw Data:** Any worksheets, records, memoranda, notes, or exact copies thereof that are the result of original observations, measurements, recordings, etc. of an activity, such as a study, operation, investigation, etc., and are necessary for the reconstruction and evaluation of the report of that activity.
- In the event that exact transcripts of raw data have been prepared (e.g., tapes which have been transcribed verbatim, dated, and verified accurate by signature), the exact copy or exact transcript may be substituted for the original source as raw data.
- Raw data may include photographs, microfilm or microfiche copies, computer printouts, magnetic media, dictated observations, and recorded data from automated instruments. As such, the raw data may exist in either hard/paper copy or electronic format.

- **Record:** (ISO) a group of related data elements treated as a unit.
- **Record Lifecycle:** The stages through which a record passes during its life. Typically, these are: Creation, Active Use, Semi-Active/Inactive Use, and Final Disposition (such as deletion).
- **Record of Change :** Documentation of changes made to the system. A record of change can be a written document or a database. Normally there are two associated with a computer system, hardware and software. Changes made to the data are recorded in an audit trail.
- **Record Retention:** (ISO) Storing and retaining quality records in an established and recorded period of time in such a way that they are readily retrievable in facilities that provide a suitable environment to prevent damage or deterioration and to prevent loss. Records may be in the form of any type of media, such as hard copy or electronic media.
- **Recovery:** Loading of backed-up data onto a computer system to recover from a problem.



As per WHO GDocP&DI guideline

- good data and record management practices. The totality of organized measures that should be in place to collectively and individually ensure that data and records are secure, attributable, legible, traceable, permanent, contemporaneously recorded, original and accurate and that if not robustly implemented can impact on data reliability and completeness and undermine the robustness of decision-making based upon those data records.



Data Integrity Principles: ALCOA

Data Integrity



EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Data integrity: key to public health protection

To ensure the integrity of data that are generated in the process of testing, manufacturing, packaging, distribution and monitoring of medicines.

Controlling of data records helps ensure that the data generated are accurate and consistent to support good decision making by both pharmaceutical manufacturers and regulatory authorities.

www.sandrarumiano.com

Ensuring Data Integrity Through ALCOA

- The acronym ALCOA has been around since the 1990's, is used by regulated industries as a framework for ensuring data integrity, and is key to Good Documentation Practice (GDP).
- ALCOA relates to data, whether paper or electronic, and is defined by WHO, EMA, UK, FDA guidance as Attributable, Legible, Contemporaneous, Original and Accurate.
- These simple principles should be part of your data life cycle, GDP and data integrity initiatives.
 - Data integrity and access control issues featured heavily within the warning letters issued by the FDA in 2015 so here is a timely refresh on the fundamentals.

Data Integrity : ALCOA

Attributable	Who performed an action and when? If a record is changed, who did it and why? Link to the source data.
Legible	Data must be recorded permanently in a durable medium and be readable.
Contemporaneous	The data should be recorded at the time the work is performed and date / time stamps should follow in order
Original	Is the information the original record or a certified true copy?
Accurate	No errors or editing performed without documented amendments.

www.sandrarumiano.com

Attributable

- ✓ All data generated or collected must be attributable to the person generating the data.
- ✓ This should include who performed an action and when.
- ✓ This can be recorded manually by initialing and dating a paper record or by audit trail in an electronic system.

signature log vs external staff

For example:

Validation exercise test results
Adjustment of a setpoint on a process or monitoring system
A correction on a lab record

Legible

- ✓ All data recorded must be legible (readable) and permanent.
- ✓ Ensuring records are readable and permanent assists with its accessibility throughout the data lifecycle.
- ✓ This includes the storage of human-readable metadata that may be recorded to support an electronic record.

For example:

GDP will always promote the use of indelible ink when completing records. When making corrections to a record, ensure a single line is used to strike out the old record. This ensures the record is still legible. Controlling your paper records/forms and formatting them such that there is ample room for the information to be recorded.

Contemporaneous

- ✓ Contemporaneous means to record the result, measurement or data at the time the work is performed.
- ✓ Date and time stamps should flow in order of execution for the data to be credible.
- ✓ Data should never be back dated.

For example:

If executing a validation protocol, tests should be performed and their results recorded as they happen on the approved protocol. Data that is logged, or testing that is performed electronically, should have a date/time stamp attached to the record. Ensure electronic systems that log data have their system clocks synchronized.

Original

Original data, sometimes referred to as source data or primary data, is the medium in which the data point is recorded for the first time. This could be a database, an approved protocol or form, or a dedicated notebook. It is important to understand where your original data will be generated so that its content and meaning are preserved.

For example:

Ensure validation test results are recorded on the approved protocol. **Recording results in a notebook for transcription later can introduce errors.**

If your original data is hand written and needs to be stored electronically, ensure a "true copy" is generated, the copy is verified for completeness and then **migrated into the electronic system.**

Accurate

- ✓ **For data and records to be accurate, they should be free from errors, complete, truthful** and reflective of the observation.
- ✓ Editing should not be performed without documenting and annotating the **amendments.**

For example:

Use a witness check for critical record collection to confirm accuracy of data.

Consider how to capture data electronically and verify its accuracy.

Build accuracy checks into the design of the electronic system.

Place controls/verification on manual data entry, for example, temperature results can only be entered within a predefined range of 0-100°C.

How you can assure your data record, traceability, integrity? You have to

- Ensure senior management leadership for data integrity:
 - Management should create a work environment in which staff are encouraged to communicate failures and mistakes
 - By ensuring adequate information flow between staff at all levels.
 - To avoid hierarchical constraints and blame cultures.
- Establishing KPIs/Quality Metrics: including Management reviews and regular reporting including a designation of a quality manager who has direct access to the highest level of management and can directly communicate risks, so that senior management is made aware of any issues and can allocate resources to address them
- Allocate a data owner for manual and computerized data processes

How you can assure your data record, traceability, integrity? To establish

- Risk assessment to identify and manage regulatory records
- Write policies and procedures for data integrity
- Ensure effective data integrity training to ensure the procedures above are followed
- Create a no-blame culture around data integrity—own up to a mistake, don't cover it up
- Establish a confidential and open, clear, not afraid, avenue for staff to communicate issues to senior management
- Management governance and quality audits
 - Effective internal data integrity audits

How you can assure your data record, traceability, integrity? To establish

- Tracking and trending of invalid and aberrant data : **APQR**
- Validation of processes, training of personnel about data source and administration
- Review of audit trails, including those reviewed as part of key decision-making steps (e.g. GMP batch release, issuance of a GLP study report or approval of case report forms)
- Routine audits and/or self-inspections of computerized systems may reveal gaps in security controls that inadvertently allow personnel: ie HPLC case
- To be aware of access and potentially alter time/date stamps
- **In case of third parties:** monitoring of contract acceptors and tracking and trending of associated quality metrics for these sites to identify risks that may indicate the need for more active engagement and allocation of additional resources by the contract giver to ensure quality standards are met.

How you can assure your data record, traceability, integrity? To implement and assure

- How Document management is done
 - Review vs revise
- How is done the archiving
- Who is in charge of the archiving
- Data entry: knowledge about data that she or he are entering
- To be committed to Good documentation practices and data integrity by your self behavior: you must be an example

How you can assure your data record,
traceability, integrity? **Something is forbidden!!!!**
Video of signature out of time



How should be completed
documento at
Bio /Pharma Industry?

Yes!!!!

- Clear content that allows the reader to interpret the process described.
- The documents should not be modified without prior authorization in the framework of the Quality System
- Documents should not be overwritten or contain handwritten annotations or clarifications that escape the original content
- When documents require data recording, they must be clear, legible, indelible blue

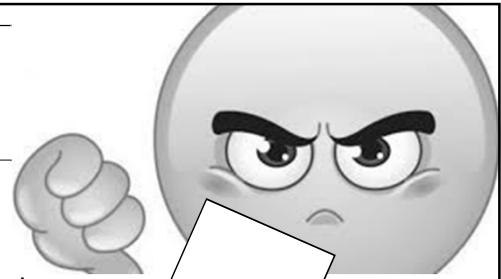
www.sandrarumiano.com

Yes!!!!

- Any correction made to a document must be made by crossing a line on the wrong data, clearly writing the correct data and signing and dating at the time the correction is made.
- Records must be made or completed at the time an action is taken so that processes are traceable. The date and responsibility must be clearly identified
- Documents must be available at the place of use and at all times when required

www.sandrarumiano.com

NO!!!!!!!!!!



- Lack of traceability
- Complete and sign with date not real
- Use expired documents
- Modify processes without modifying accompanying documents
- Use records that do not include an SOP reference document
- Paste the records out of time

FALSIFIED DOCUMENTATION

www.sandrarumiano.com

Bases of Good documentation practices and Data Integrity

- The organisation needs to take responsibility for the systems used and the data they generate: organisational culture should ensure data is complete, consistent and accurate in all its forms, i.e. paper and electronic.
- 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, to enable data integrity controls to be effective.
- KPI are suitable to analyzed and improved the GDocP&DI: ie PQPR

Bases of Good documentation practices and Data Integrity

- Organisations are expected to implement, design and operate a documented system that provides an acceptable state of control based on the data integrity risk assessment (DIRA) **where the processes that produce data or where data is obtained are mapped out and each of the formats and their controls are identified and the data criticality and inherent risks documented.**
- Data governance measures should ensure that periodic audits can detect opportunities for data integrity failures within the organization's systems.

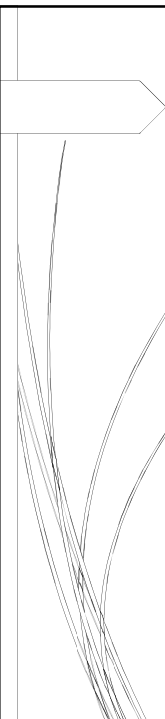
Bases of Good documentation practices and Data Integrity

- **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.
- Automated or computerized systems as well paper-based manual systems are under data integrity controls.
- Where data integrity weaknesses are identified, companies should ensure that appropriate corrective and preventive actions are implemented across all relevant activities and systems and not in isolation.



Bases of Good documentation practices and Data Integrity

- All GXP records held by the GXP organization are subject to inspection by the responsible health authorities.
 - This includes original electronic data and metadata, such as audit trails maintained in computerized systems.
- Management of both contract givers and contract acceptors should ensure that adequate resources are available and that procedures for computerized systems are available for inspection.
- System administrator personnel should be available to readily retrieve requested records and facilitate inspections.



Good documentation practices and Data Integrity Guidelines

Data integrity: Not a new concept: FDA Principles from the paper-and-ink era still apply:

- 211.68 requires that backup data are exact and complete, and secure from alteration, inadvertent erasures, or loss.
- 212.110(b) requires that data be stored to prevent deterioration or loss.
- 211.100 and 211.160 require that certain activities be documented at the time of performance and that laboratory controls be scientifically sound.
- 211.180 requires true copies or other accurate reproductions of the original records; and
- 211.188, 211.194, and 212.60(g) require complete information, complete data derived from all tests, complete record of all data, and complete records of all tests performed.

8

API - ICH Q7

Computerized systems (5.4):

- Computerized systems should have sufficient controls to prevent unauthorized access or changes to data. There should be controls to prevent omissions in data (e.g., system turned off and data not captured). There should be a record of any data change made, the previous entry, who made the change, and when the change was made.
- If system breakdowns or failures would result in the permanent loss of records, a back-up system should be provided. A means of ensuring data protection should be established for all computerized systems.

Q7 Good Manufacturing Practice Guidance for Active Pharmaceutical Ingredients

API - ICH Q7

Computerized systems (5.4):

- GMP-related computerized systems should be validated.
- Appropriate installation and operational qualifications should demonstrate the suitability of computer hardware and software to perform assigned tasks.
- Incidents related to computerized systems that could affect the quality of intermediates or API or the reliability of records or test results should be recorded and investigated.

Q7 Good Manufacturing Practice Guidance for Active Pharmaceutical Ingredients

Coming now specific and
strong Guidelines on
Good documentation
practices
and Data Integrity

WHO Data Integrity WHO_TRS_996_annex05

► Guidance on good data and record management practices

Annex 5

Guidance on good data and record management practices

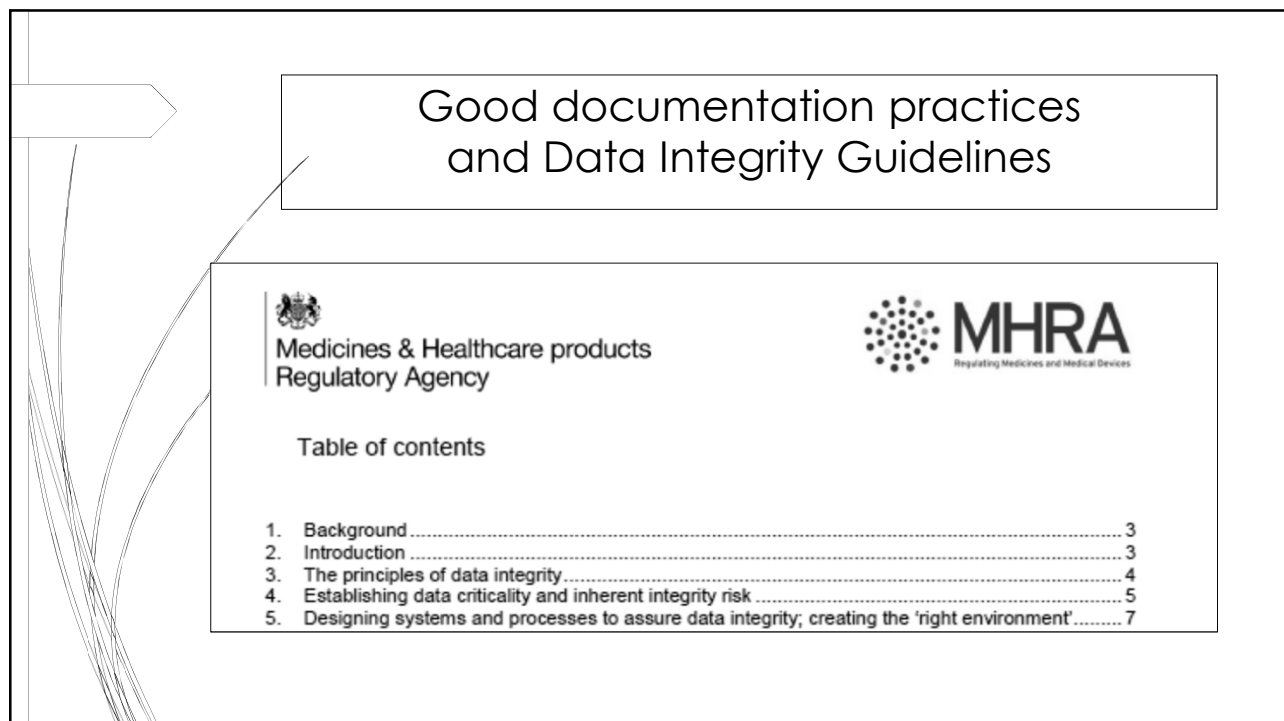
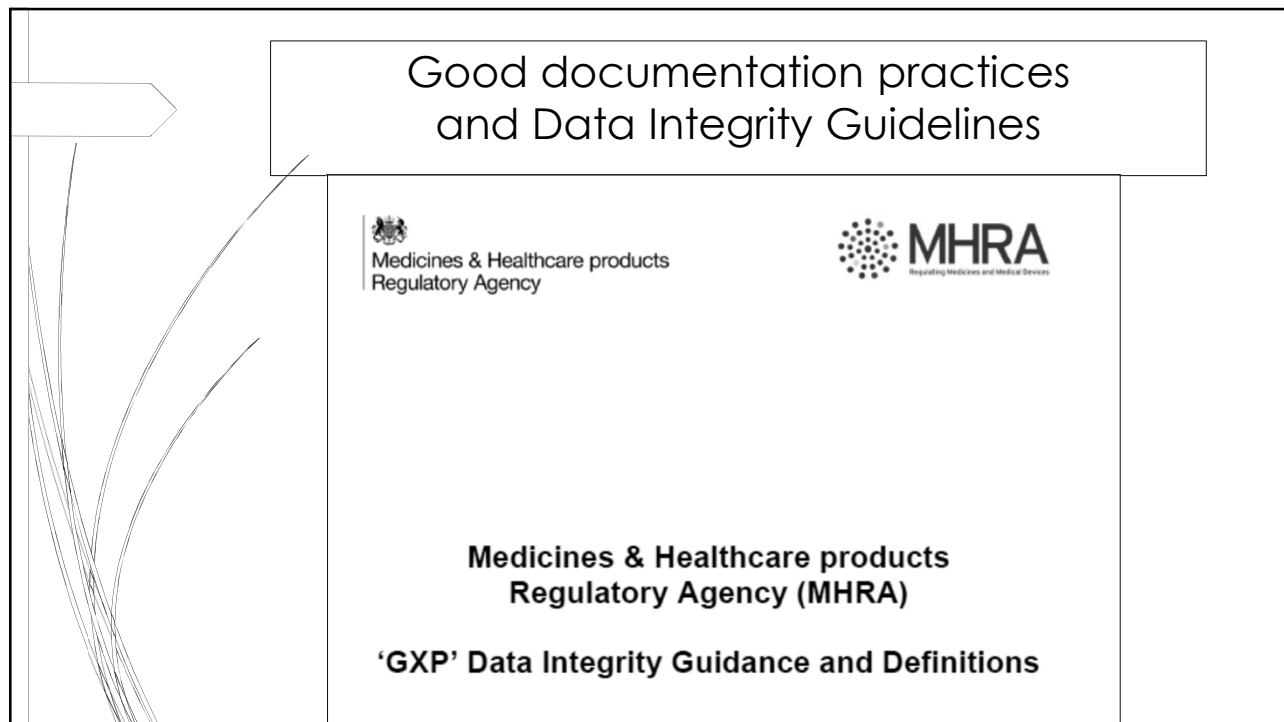
1. Introduction	167
2. Aims and objectives of this guidance	169
3. Glossary	169
4. Principles	173

WHO Data Integrity WHO_TRS_996_annex05

► Guidance on good data and record management practices

4. Principles
5. Quality risk management to ensure good data management
6. Management governance and quality audits
7. Contracted organizations, suppliers and service providers
8. Training in good data and record management
9. Good documentation practices
10. Designing and validating systems to assure data quality and reliability
11. Managing data and records throughout the data life cycle
12. Addressing data reliability issues

www.sandrarumian.com



Good documentation practices and Data Integrity Guidelines

6. Definition of terms and interpretation of requirements.....	8
6.1. Data	8
6.2. Raw data (synonymous with 'source data' which is defined in ICH GCP)	8
6.3. Metadata	9
6.4. Data Integrity.....	9
6.5. Data Governance.....	9
6.6. Data Lifecycle.....	10
6.7. Recording and collection of data	10
6.8. Data transfer / migration	10
6.9. Data Processing.....	11
6.10. Excluding Data (not applicable to GPvP):	11
6.11. Original record and true copy.....	11
6.11.1. Original record	11
6.11.2. True copy	12
6.12. Computerised system transactions:	13
6.13. Audit Trail	13
6.14. Electronic signatures.....	14
6.15. Data review and approval	15
6.16. Computerised system user access/system administrator roles	16
6.17. Data retention	17
6.17.1. Archive	18
6.17.2. Backup	18
6.18. File structure.....	19
6.19. Validation – for intended purpose (GMP; See also Annex 11, 15).....	19
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)).	19
7. Glossary	20
8. References.....	21



EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Good documentation practices and Data Integrity Guidelines


Data integrity (NEW August 2016)

[Back to top](#)

[Expand all items in this list](#)

Data integrity

- [1. How can data risk be assessed?](#)
- [2. How can data criticality be assessed?](#)
- [3. What does 'Data Lifecycle' refer to?](#)
- [4. Why is 'Data lifecycle' management important to ensure effective data integrity measures?](#)
- [5. What should be considered when reviewing the 'Data lifecycle'?](#)
- [6. 'Data lifecycle': What risks should be considered when assessing the generating and recording of data?](#)
- [7. 'Data lifecycle': What risks should be considered when assessing the processing data into usable information?](#)
- [8. 'Data lifecycle': What risks should be considered when checking the completeness and accuracy of reported data and processed information?](#)
- [9. 'Data lifecycle': What risks should be considered when data \(or results\) are used to make a decision?](#)
- [10. 'Data lifecycle': What risks should be considered when retaining and retrieving data to protect it from loss or unauthorised amendment?](#)
- [11. 'Data lifecycle': What risks should be considered when retiring or disposal of data in a controlled manner at the end of its life?](#)



EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Good documentation practices and Data Integrity Guidelines

What risks should be considered when retiring or disposal of data in a controlled manner at the end of its life?

12. Is it required by the EU GMP to implement a specific procedure for data integrity?

13. How are the data integrity expectations (ALCOA) for the pharmaceutical industry prescribed in the existing EU GMP relating to active substances and dosage forms published in Eudralex volume 4?

14. How should the company design and control their paper documentation system to prevent the unauthorised re-creation of GMP data?

15. What controls should be in place to ensure original electronic data is preserved?

16. Why is it important to review electronic data?

17. Is a risk-based review of electronic data acceptable?

18. What are the expectations for the self-inspection program related to data integrity?


19. What are my company's responsibilities relating to data integrity for GMP activities contracted out to another company?

20. How can a recipient (contract giver) build confidence in the validity of documents such as Certificate of Analysis (CoA) provided by a supplier (contract acceptor)?

21. What are the expectations in relation to contract calibration service providers who conduct calibrations on-site and/or off-site? Are audits of these companies premises required?

22. What is expected of my company in the event that one of my approved contractors (e.g. active substance manufacturer, finished product manufacturer, quality control laboratory etc.) is issued with a warning letter/statement of non-compliance concerning data integrity, from a regulatory authority?

23. Where does my company's responsibility begin and end in relation to data integrity aspects of the supply chain for medicinal products?



Publications

Since its creation, PIC/S has been active in the development and promotion of harmonised GMP standards and guidance documents.

The main instrument for harmonisation has been the PIC/S GMP Guide. Originally, the latter derives from the WHO GMP Guide and has been further developed in order to comply with stringent manufacturing and health requirements, to cover new areas (e.g. biologicals) and to adapt to scientific and industrial technology (e.g. biotech).

In 1989, the EU adopted its own GMP Guide, which - in terms of GMP requirements - is equivalent to the PIC/S GMP Guide. Since that time, the EU and the PIC/S GMP Guides have been developed in parallel (both Guides are practically identical).

In addition to the GMP Guide, PIC/S has also been a pioneer in developing a number of guidelines and guidance documents such as the Site Master File, the Recommendation on Quality System Requirements for Pharmaceutical Inspectors and the first Guideline for the Manufacture of Active Pharmaceutical Ingredients. As a matter of fact, PIC/S has been instrumental in elaborating a first draft for the ICH Q7A Guide on APIs, which was finalised by ICH in 2000 and then adopted by PIC/S.

All PIC/S documents publicly available are listed below and appear in alphabetical order. Protected documents are for PIC/S Members-only and require a login.

Good
documentation
practices
and Data Integrity
Guidelines

All
GMP Guide
Latest
Drafts
Protected

Category ▼ | Section ▼

* Draft	Reference	Category	Section
CONSULTATION DOCUMENT ON ANNEX 1 (MANUFACTURE OF STERILE MEDICINAL PRODUCTS)	Consultation Document on Revision of Annex 1	Documents for industry	PIC/S GMP Guide
DRAFT PIC/S GOOD PRACTICES FOR DATA MANAGEMENT AND ITS ASSOCIATED INFORMATION TECHNOLOGY SYSTEMS	PI 041-1 (Draft 2)	Documents for inspectors	Guidance documents

Good documentation practices and Data Integrity Guidelines



PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 041-1 (Draft 2)
10 August 2016

DRAFT PIC/S GUIDANCE

GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED
GMP/GDP ENVIRONMENTS

© PIC/S August 2016
Reproduction prohibited for commercial purposes.
Reproduction for internal use is authorised,
provided that the source is acknowledged.

Editor: PIC/S Secretariat

e-mail: info@picscheme.org

web site: <http://www.picscheme.org>

Good documentation practices and Data Integrity Guidelines

TABLE OF CONTENTS

	Page
1. Document history	3
2. Introduction	3
3. Purpose	4
4. Scope	5
5. Data governance system	5
5.1 What is data governance	5
5.2 Data governance systems	5
5.3 Risk management approach to data governance	6
5.4 Data criticality	6
5.5 Data risk	7
5.6 Data governance system review	7
6. Organisational influences on successful data integrity management	8
6.1 General	8
6.2 Code of ethics and policies	9
6.3 Quality culture	10
6.4 Modernising the Pharmaceutical Quality Management System	10
6.5 Regular management review of quality metrics	10
6.6 Resource allocation	10
6.7 Dealing with data integrity issues found internally	11
7. General data integrity principles and enablers	11
8. Specific data integrity considerations for paper-based systems	13
8.1 Structure of QMS and control of blank forms/templates/records	13
8.2 Why is the control of records important?	14
8.3 Generation, distribution and control of template records	14
8.4 Expectations for the generation, distribution and control of records	14
8.5 Use and control of records within production areas	16
8.6 Filing out records	16
8.7 Making corrections on records	18
8.8 Verification of records	18
8.9 Maintaining records	19
8.10 Direct print-outs from electronic systems	20
8.11 True copies	20
8.12 Limitations of remote review of summary reports	21
8.13 Document retention	21
8.14 Disposal of original records	22
9. Specific data integrity considerations for computerised systems	23
9.1 Structure of QMS and control of computerised systems	23
9.2 Qualification and validation of computerised systems	23
9.3 System security for computerised systems	27
9.4 Audit trails for computerised systems	29
9.5 Data capture/entry for computerised systems	30

Good documentation practices and Data Integrity Guidelines

9.6	Review of data within computerised systems.....	32
9.7	Storage, archival and disposal of electronic data.....	33
10.	Data Integrity considerations for outsourced activities	35
10.1	General supply chain considerations	35
10.2	Routine document verification.....	35
10.3	Strategies for assessing data integrity in the supply chain	35
11.	Regulatory actions in response to data integrity findings	37
11.1	Deficiency references.....	37
11.2	Classification of deficiencies.....	37
12.	Remediation of data integrity failures	38
12.1	Responding to significant data integrity issues	38
12.2	Indicators of improvement.....	40
13.	Definitions	40
14.	Revision history.....	41



Good documentation practices and Data Integrity Guidelines

Data Integrity and Compliance With CGMP Guidance for Industry

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Veterinary Medicine (CVM)

April 2016
Pharmaceutical Quality/Manufacturing Standards (CGMP)



Good documentation practices and Data Integrity Guidelines

Contains Nonbinding Recommendations

Draft — Not for Implementation

TABLE OF CONTENTS

I. INTRODUCTION	1
II. BACKGROUND	1
III. QUESTIONS AND ANSWERS	2
1. Please clarify the following terms as they relate to CGMP records:	2
a. What is "data integrity"?	2
b. What is "metadata"?	3
c. What is an "audit trail"?	3
d. How does FDA use the terms "static" and "dynamic" as they relate to record formats?	3
e. How does FDA use the term "backup" in § 211.68(b)?	4
f. What are the "systems" in "computer or related systems" in § 211.68?	4
2. When is it permissible to exclude CGMP data from decision making?	4
3. Does each workflow on our computer system need to be validated?	4
4. How should access to CGMP computer systems be restricted?	5
5. Why is FDA concerned with the use of shared login accounts for computer systems?	6
6. How should blank forms be controlled?	6
7. How often should audit trails be reviewed?	6
8. Who should review audit trails?	6
9. Can electronic copies be used as accurate reproductions of paper or electronic records?	7
10. Is it acceptable to retain paper printouts or static records instead of original electronic records from stand-alone computerized laboratory instruments, such as an FT-IR instrument?	7
11. Can electronic signatures be used instead of handwritten signatures for master production and control records?	8
12. When does electronic data become a CGMP record?	8
13. Why has the FDA cited use of actual samples during "system suitability" or test, prep, or equilibration runs in warning letters?	9
14. Is it acceptable to only save the final results from reprocessed laboratory chromatography?	9
15. Can an internal tip regarding a quality issue, such as potential data falsification, be handled informally outside of the documented CGMP quality system?	9
16. Should personnel be trained in detecting data integrity issues as part of a routine CGMP training program?	10
17. Is the FDA investigator allowed to look at my electronic records?	10
18. How does FDA recommend data integrity problems identified during inspections, in warning letters, or in other regulatory actions be addressed?	10



Data Reliability Guideline

February 2017

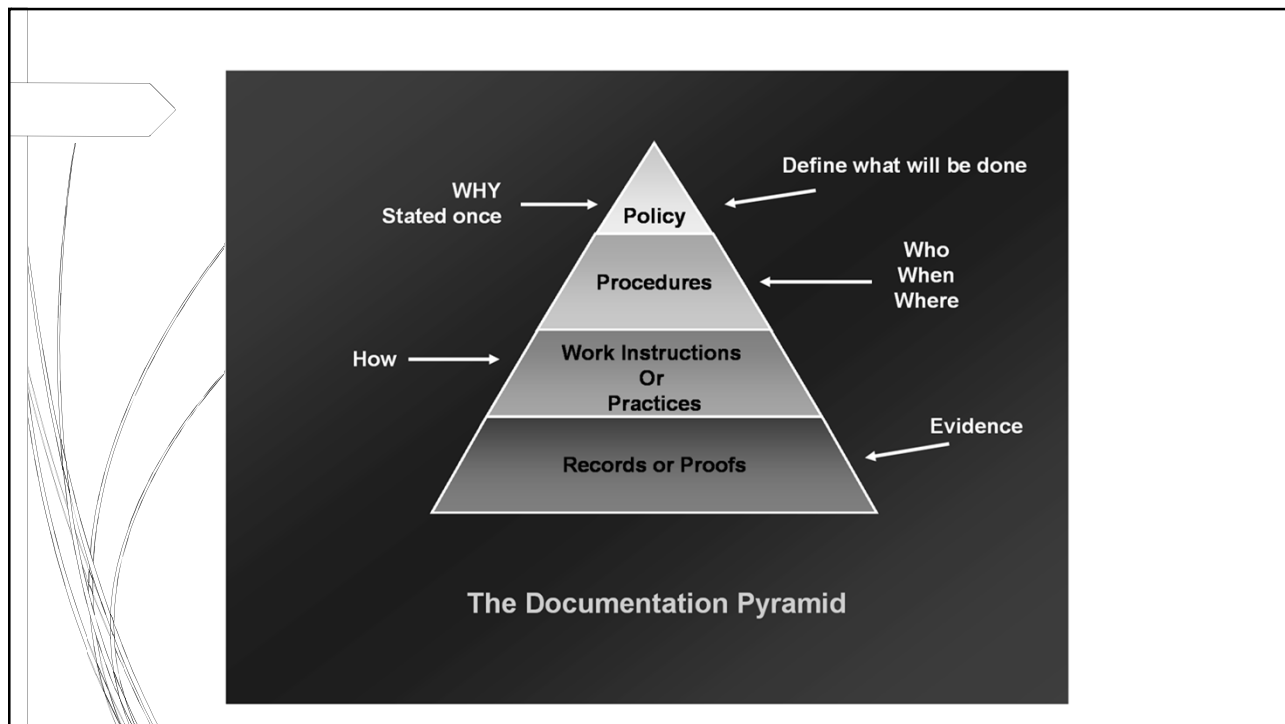


Data Reliability Guideline



Implementation of Data Integrity Standards at your Site

- Management should take responsibility for good data management by first setting realistic and achievable expectations for the true and current capabilities of a process, a method, an environment, personnel, or technologies, among others
- Management must encourage ethics and trust, avoiding fear of making mistakes
- The Monitoring of processes and their related documentation should be established in SOPs/Policy's, etc. and Responsible must be identified and assume their responsibilities
- To provide training for personnel, assuring that GDocP&DI is understood in order to take care of the Health of the Public
- To list the documents needs in accordance to regulations and establish the Documental Pyramid as well as the DI requirement
- Internal and external audits must consider GDocP&DI



QRM approach that effectively assures patient safety and product quality and validity of data by ensuring that management aligns expectations with actual process capabilities.

Data Integrity risk assessment

- assessment of risks to data integrity in the collection, processing and storage of data;
- risk management measures at various stages of the 'data lifecycle';
- design and control of both electronic and paper based documentation systems;
- measures to ensure data integrity for activities contracted out to another company.

www.sandrarumiano.com

Risk of absence of GDocP & Data Integrity:

- Health of the Public affected
- Private and Public property can be affected
- FP shortages
- Loss of consumer confidence
- Non-compliance in NRA inspections can result in financial impact:
 - Loss of Market opportunities
 - Product applications review suspended
 - Market & share price reduction

www.sandrarumiano.com

Implementation of Data Integrity Standards at your Site

To generate and record on time: raw data

To analyze and work on your raw data

To provide allowance to data & data process

To establish the time and the way for archiving documents

To establish the final disposal: how and who will be in charge of final destruction of documents

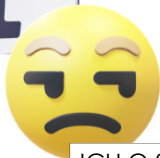
It ask for....

- adoption of a quality culture within the company that encourages personnel to be transparent
- mapping of data processes and application of modern QRM and sound scientific principles throughout the data life cycle;
- ensuring that all site personnel are kept up to date about the application of good documentation practices (GDocP) to ensure that the GXP principles of ALCOA are understood and applied to electronic data in the same manner that has historically been applied to paper records;
- implementation and confirmation during validation of computerized systems and subsequent change control, that all necessary controls for GDocP for electronic data are in place and that the probability of the occurrence of errors in the data is minimized;
- training of personnel who use computerized systems and review electronic data in basic understanding of how computerized systems work and how to efficiently review the electronic data, which includes metadata and audit trails;
- definition and management of appropriate roles and responsibilities for quality agreements and contracts entered into by contract
- givers and contract acceptors, including the need for risk-based monitoring of data generated and managed by the contract acceptor on behalf of the contract giver;
- modernization of quality assurance inspection techniques and gathering of quality metrics to efficiently and effectively identify risks and opportunities to improve data processes.

The GMP Document Roadmap: Implementation model based on Quality Risk Management

sor2

Road to Compliance: GAP analysis



ICH Q 8: product & process understanding



ICH Q 10: Pharmaceutical Quality System

ICH Q 9 Quality Risk Management



Yes! We did!!!!

Diapositiva 58

sor2 sandra olga rumiano, 02/06/2018

ICH Q8(R2) – Pharmaceutical Development Related Activities	ICH Q9 – QRM Related Activities	ICH Q10 – PQS Related Integrated Activities
<ul style="list-style-type: none"> • Gain product and process knowledge • Knowledge supports transfer between development and manufacturing to achieve product realization 	<ul style="list-style-type: none"> • Forms the basis for the manufacturing process • Improves effectiveness of control strategy • Contributes to processes validation and ongoing continual improvement 	<ul style="list-style-type: none"> • Advance understanding through scale-up activities • Provide preliminary indication of process performance and successful integration into manufacturing • Gain knowledge from transfer and scale up activities to enhance the basis for the control strategy

Source: ICH-Presentation-on-Q8-9-10

Applying ICH Q 8

The aim of pharmaceutical development is to design a quality product and its manufacturing process to consistently deliver the intended performance of the product.

Quality cannot be tested into products: quality should be built into product

Information from pharmaceutical development studies can be a basis for Quality Risk Management

The scope is to:
To avoid simplicity and approach
Enhanced knowledge approach



Paper and electronic data

■ Paper

- Data generated manually on paper may require independent verification if deemed necessary from the data integrity risk assessment or by another requirement.
- Consideration should be given to risk-reducing supervisory measures.


■ Electronic


- The inherent risks to data integrity relating to equipment and computerised systems may differ depending upon the degree to which the system generating or using the data can be configured, **and the potential for manipulation of data during transfer between computerised systems during the data lifecycle.**

Data process maps for paper and hybrid process

Handling hybrid records: Good Documentation Practices for linked paper and electronic records

- Chapter 4 and 21 CFR 11 regulations for linking signatures to electronic records
- Checks and technical controls to ensure the signature is linked to the record as legal profile
- Master Document Control
- Second Person Review of Batch and analytical records: paper, hybrid and electronic formats: review on paper, hybrid and electronic records
 - Risk based second person reviews of records and audit trails challenge
- Validations & Verification: Risk Assessment as Base of Period Definition

	<p>Data process maps for paper and hybrid process</p>
<p>Handling hybrid records: Good Documentation Practices for linked paper and electronic records</p> <ul style="list-style-type: none"> ➤ Hybrid ➤ Where hybrid systems are used, it should be clearly documented what constitutes the whole data set and all records that are defined by the data set should be reviewed and retained. Hybrid systems should be designed to ensure they meet the desired objective. 	

	<p>Data process maps for paper and hybrid process</p>
<p>Handling hybrid records: Good Documentation Practices for linked paper and electronic records</p> <ul style="list-style-type: none"> ➤ Other ➤ Where the data generated is captured by a photograph or imagery (or other media), the requirements for storage of that format throughout its lifecycle should follow the same considerations as for the other formats, considering any additional controls required for that format. Where the original format cannot be retained due to degradation issues, alternative mechanisms for recording (e.g. photography or digitisation) and subsequent storage may be considered and the selection rationale documented (e.g. thin layer chromatography). 	

You have to assure

- Computer system validation
- Establish procedures for Backup and Recovery System: who is in charge? How?
- Security controls:
 - Physical
 - Separated areas
 - Biometrics devices for entering different areas
- IT/Cyber security:
 - it is allowed to discharged from Internet any application/softw?
 - Virus protection
 - ID and passwords control
 - Open PC time



TIME FOR
LUNCH

Exercise:
working in our
road map



Some points for building your road map

- Build the road to comply with the traceability and data integrity:
 - List your Documents
 - Classified them and their owners in hard copy and electronic format
 - Establish your Gap analysis of where we are and how to build in steps and how to get to the critical points of data integrity, archiving, governance, etc.
- Consider if:
 - Is there computer security or not?
 - Do you have Company confidentiality agreement or not??
 - Somebody can Enter with same password ???
 - Do you know if in the Company are share licenses, is there a possibility that you can enter with the password of another with permission?



3 critical points found for succeed/equipment



Pre-requisites:
data integrity policy with effective training

- Policy is a declaration that establish Upper Management and Employees commitment regards GDocP DI usually based on ALCOA principles
- This Policy must include the commitment towards train and follow up, but not only, on this principles.
- It must consider also to Company members encouraging towards Transparency and Honesty

Identifying risk to records and mitigating them

Work on

- GAP analysis about Regulatory Documents, Data and Records need and your situation
- Life Cycle requirements are reflected in your SOP of SOPs
 - Managing the life of the data (initial creation, review, approval, storage, obsolete)
- Staff training is training or just reading?
- Staff understanding level of ALCOA
- Speaking of OOS and or deviations is a problem in your Organization
- Does your Cy have a Confidentiality Agreement with employees towards data and information privacy?

Work with

► Documents:

- It is Develop a Data Integrity Policy and Procedures /Training to staff to address data ownership throughout the lifecycle?
- It is the Design, operation and monitoring of processes and their documents established and staff is tri on it?

► Management of third parties: do you Company consider

- Contracts: share to information
 - Working At site
 - Quality Agreements
- Computers use

► Do you have General security controls?

- Physical vs biometrics
- Time out/computer
- Prohibited to share password!!!!
- staff consciousness

Work in

► Internal audit process:

- including GDocP&DI
- Training and CAPA plans on GDocP&DI

► External audits for data governance

- Archiving
 - Hard copies
 - Back up electronic data
- Archivist
- Data enters
- IT suppliers
- Distribution suppliers:
 - Import and export activities documentation

How to train staff in Good Documentation Practice and Data Integrity

Assess Training Needs

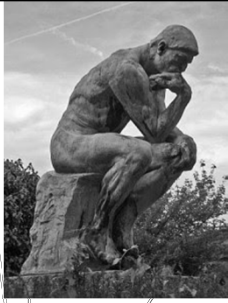
- List your documents, records.
- Evaluate the understanding on them
 - Analyze deviations trends on GDocP&DI
- Look at current training
- Consider the New regulations and Internal Policies



Set Priorities

- Fatal or serious hazards coming from lack of GDocP&DI: follow up complaints and APQR
- Major delays because of poor or incomplete documentation impacts
- Recurring misinformation during BR or another documents review
- Foundational training areas:
 - Establish the Plan & Program in detail including:
 - Participants
 - Objectives
 - Scope
 - Content
 - Q&A
 - Evaluation
 - Follow up: qualification

- Material should have immediate usefulness to the learners and be relevant to adult learners' lives.
- Training environment should be welcoming so that all learners feel safe to participate.
- Training material should be engaging allowing learners have an opportunity to share their experiences.



Individuals learn best when they are ready to learn and when they have identified their own learning needs.



www.sandrarumiano.com

- Connect to the personal interests of participants.
- Connect the content to current situations.
- Let students provide opinion on their learning behavior
- Give transparent explanation and feedback
- Use different cooperative learning formats

Invite Participation with examples: BR, analyst logbook, T/RH% record, etc

www.sandrarumiano.com

Control of Templates and Blank Forms

- Come back to the bases: SOP Of SOPs management:
 - Controlled vs uncontrolled copies
 - Excedent of copies/Xerox
 - Availability of anyone to print templates and blank forms
 - Lack of control during BR review on formats used
- Furnitures available for just in case kept copies
- Solve the problem by transcription on current version of templates
- Lack of CAPA plan application including training and follow up

Common pitfalls

- Use of posticks or flags
- Use of pencil
- Data review limited to printed records - no review of e-source data
- System admin within QC, can delete data
- DI is not only a QC lab issue
- DI awareness training/refresher absent
- DI verification not part of self inspections

Common pitfalls

- QA oversight of mistake's
- QA attitude negligible in reviewing document's
- Shared Identity/Passwords
- WARNING.. . DI contributing factors
 - Leadership and KPIs can drive wrong behaviors
 - Inappropriate system design encourage bad practices
 - Culture of fear, blame and punishment
- Poor attitude to problems- miss learning opportunities

Common pitfalls

- Don't care, won't get caught attitude
- Lack culture of quality, doing it right when nobody is watching
- Insufficiently controlled processes
- Poor documentation practices
- Suboptimal quality oversight
- Professional ignorance
- Intentional data falsification
- Old computerized systems not complying with part 11 or Annex 11



Practical Exercises :
follow up our
documentation
in Production and QC

Instructions

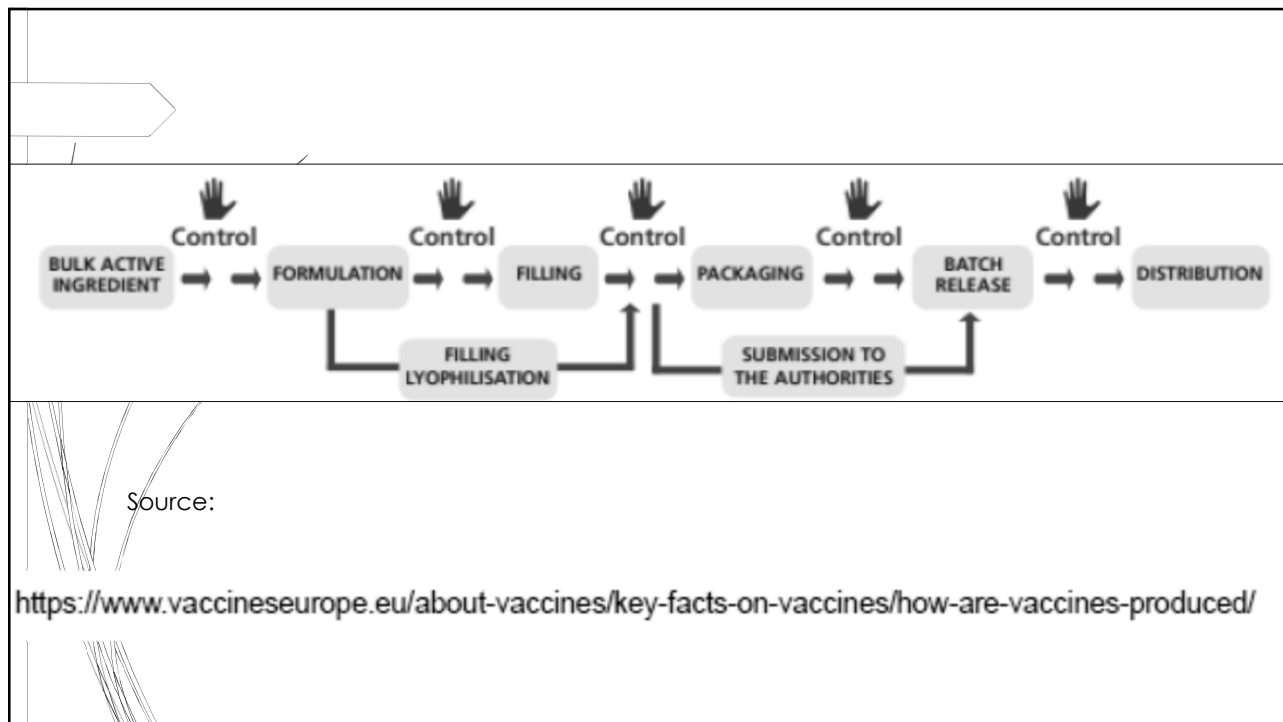
■ Starting from receiving material till dispatch and reception at final destination:

- Prepare a list base on this example or your product of your Documents in Production and QC
- List for each one the responsible/s involved
- List for each one the most common pitfalls
- Add a column to included a proposal to managed them
- Elaborate as conclusion an Action Plan

Instructions

■ You can use as example, but not only:

- BR blank format
- Analyst logbooks
- VMP
- BR review
- Complaint management





General discussion

Day 1 is
closed
Thank you!!
See you
Tomorrow
morning

