WIN AS ONE

Preparing for a Data Integrity (DI) Audit

Garry Wright

European Laboratory Compliance Specialist

Apollo Hotel, Breda – 2nd February 2016

garry.wright@agilent.com

Agenda

- Data Integrity / Data Life Cycle?
- Data Integrity Statistics.
- Example Data Integrity Warning Letter.
- Quality Culture.
- Good Documentation Practice (GDP - ALCOA).
- New approach to audit.
- Data Integrity - Audit Preparation.
- Data Integrity - Risk Assessment.
- Data Integrity - Procedures / SOP's.
- IT Infrastructure.
- Administration.
- Data Management.
- Data Processing.
- Data Review (Internal / External).
- Anti-Fraud auditing.

WIN AS ONE

Data Integrity / Data Life Cycle?

Data Integrity / Data Life Cycle?

Data Integrity

The extent to which all data are complete, consistent and accurate throughout the data life cycle.

Data Life Cycle

The data life cycle covers data generation, processing, reporting, archival, retrieval and destruction.

Source : MHRA Regulating Medicines and Medical Devices Data Integrity Definition Guidance (Mar 2015)

WIN AS ONE

Data Integrity Statistics

Data Integrity Statistics

U.S. Food and Drug Administration
Protecting and Promoting *Your* Health

A to Z Index | Follow FDA | En Español

SEARCH

Home | Food | Drugs | Medical Devices | Radiation-Emitting Products | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Tobacco Products

FDA's Electronic Reading Room - Warning Letters

FDA Home ◉ Warning Letters and Responses ◉ Warning Letters Search Results

Data integrity

210 WL's
2005 - 2015

Warning Letters Search Results

Search all warning letters

data integrity | Search | Advanced Search

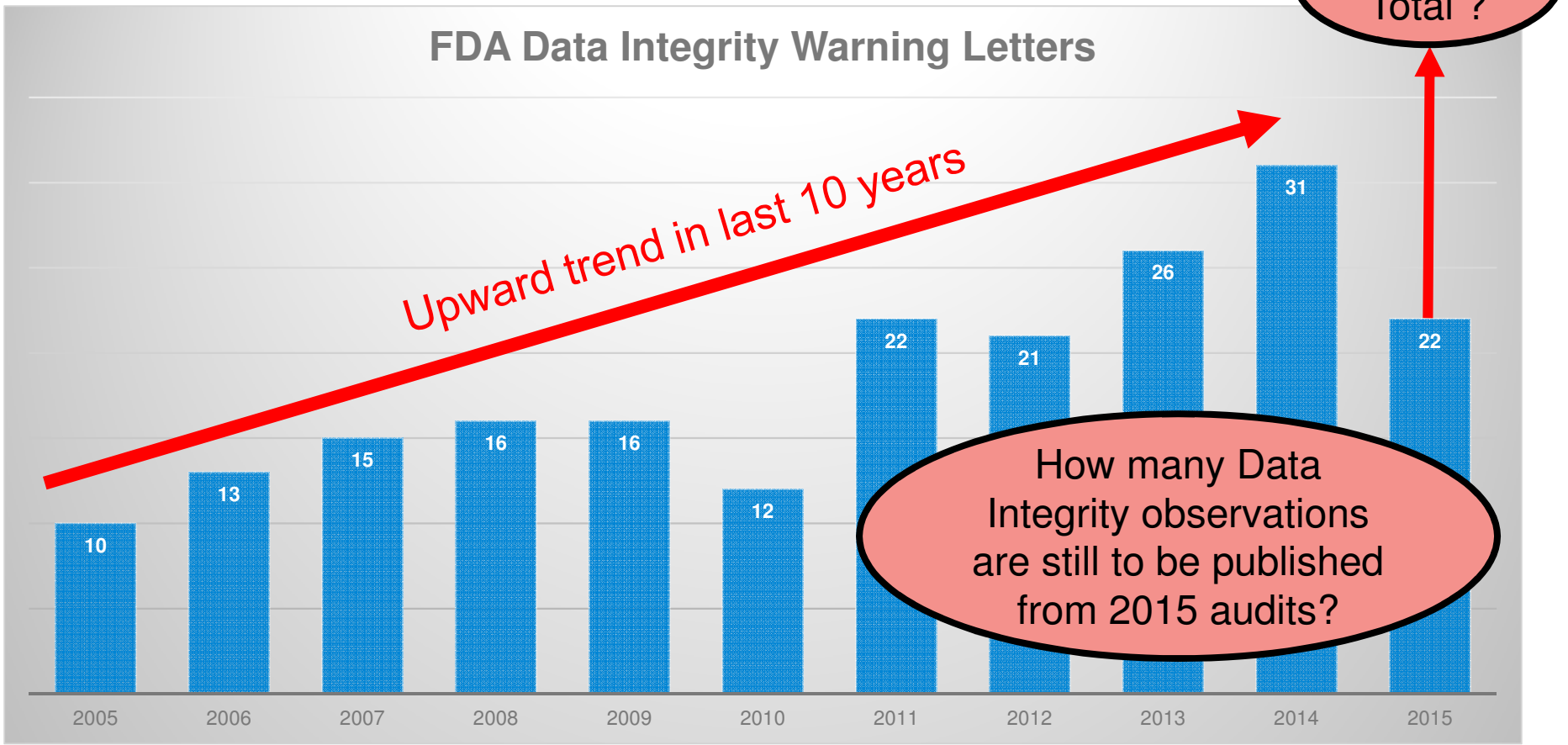
Sort by: Letter Issued DESC | Go | Reset

No. of Letters Found: 210

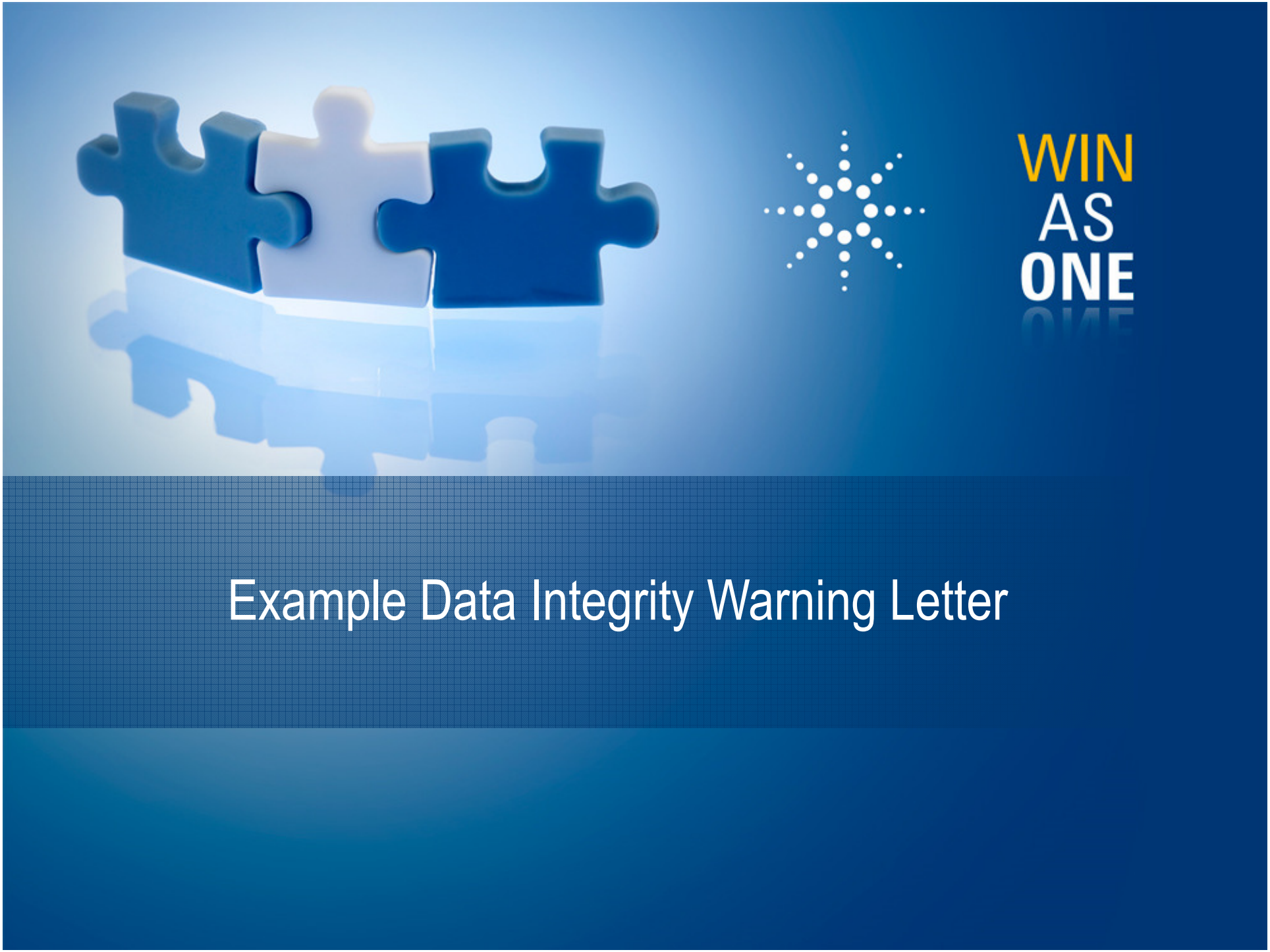
Company	Letter Issued	Issuing Office	Subject	Response Letter Posted	Closeout Date
Zhejiang Hisun Pharmaceutical Co., Ltd.	12/31/2015	Center for Drug Evaluation and Research	CGMP/Active Pharmaceutical Ingredient (API)/Adulterated	No	
Cadila Healthcare Limited	12/23/2015	Center for Drug Evaluation and Research	CGMP/Active Pharmaceutical Ingredient (API)/Adulterated	No	
Dr. Reddy's Laboratories Limited	11/05/2015	Center for Drug Evaluation and Research	CGMP/Active Pharmaceutical Ingredient (API)/Adulterated	No	
Triangle Compounding	11/02/2015	Atlanta District Office	CGMP/Finished Pharmaceuticals/Adulterated	No	
Sandoz Private Limited	10/22/2015	Center for Drug Evaluation and Research	CGMP/Active Pharmaceutical Ingredient (API)/Adulterated	No	
Unimark Remedies Ltd.	09/28/2015	Center for Drug Evaluation and Research	CGMP/Active Pharmaceutical Ingredient (API)/Adulterated	No	
Mylan Laboratories Limited	08/06/2015	Center for Drug Evaluation and Research	CGMP/Finished Pharmaceuticals/Adulterated	No	
Mahendra Chemicals	07/13/2015	Center for Drug Evaluation and Research	CGMP/Finished Pharmaceuticals/Adulterated	No	

Source: www.fda.gov

Data Integrity Statistics



- Based on Warning Letter issue date.
- Majority of 2015 WL's from audits performed in 2014.



Example Data Integrity Warning Letter

Example Data Integrity Warning Letter

- FDA Warning Letter issued 5 Nov 2015.
- Generics Pharma company.
- 3 sites in India audited between Nov 2014 and Mar 2015.

Warning letter took 8 months to issue due to 18 observations and high level of detail included based on severity of findings!

"No user specific passwords for HPLC systems".

"No audit trail".

"Users have full access".

"Data not documented in real-time".

"Ability to change / delete electronic raw data".

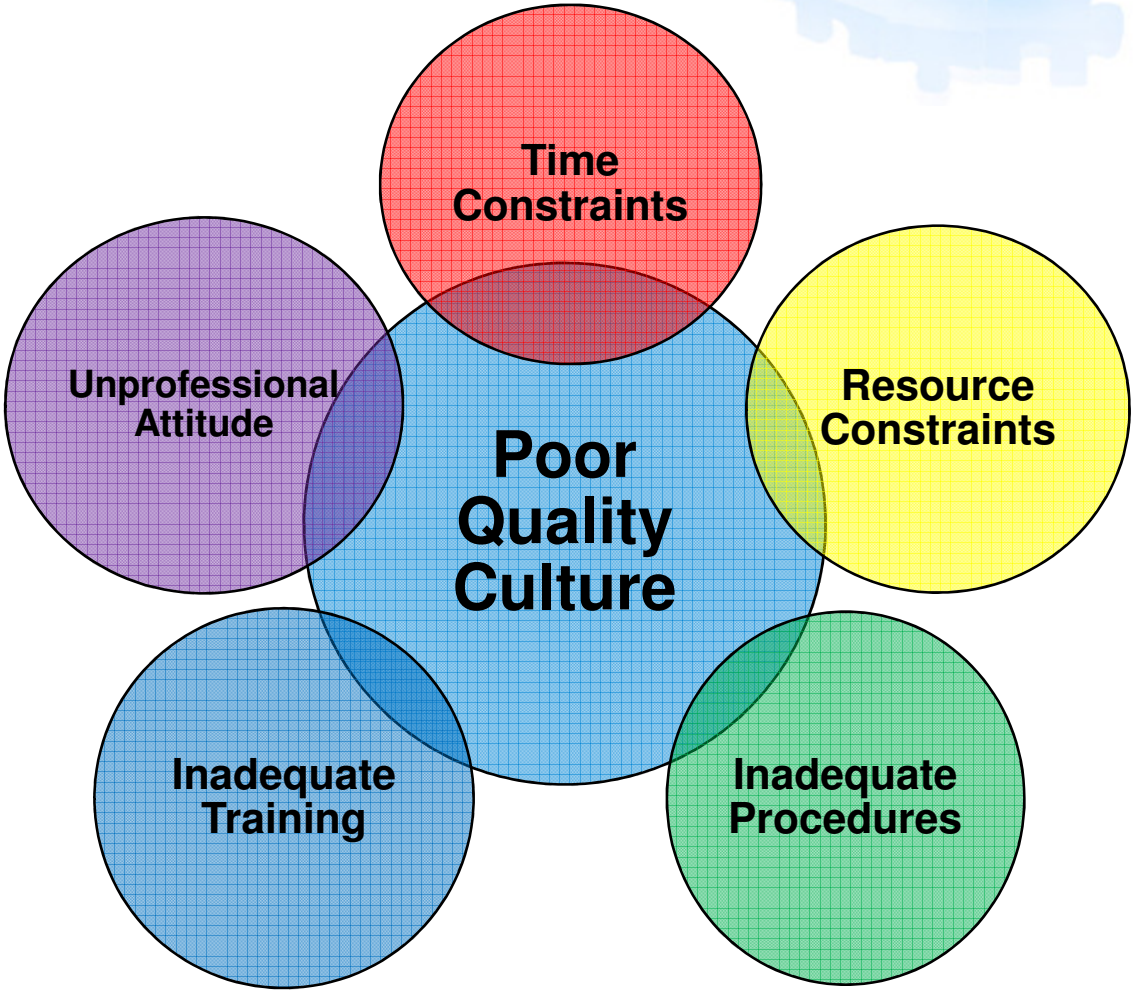
"Results recorded on un-official documents".

"Failure to maintain complete data".

Quality Culture

Quality Culture

- Data integrity issues occur and are identified by auditors as a direct result of poor quality culture within organisations.



Quality culture needs to be promoted throughout the whole organisation!

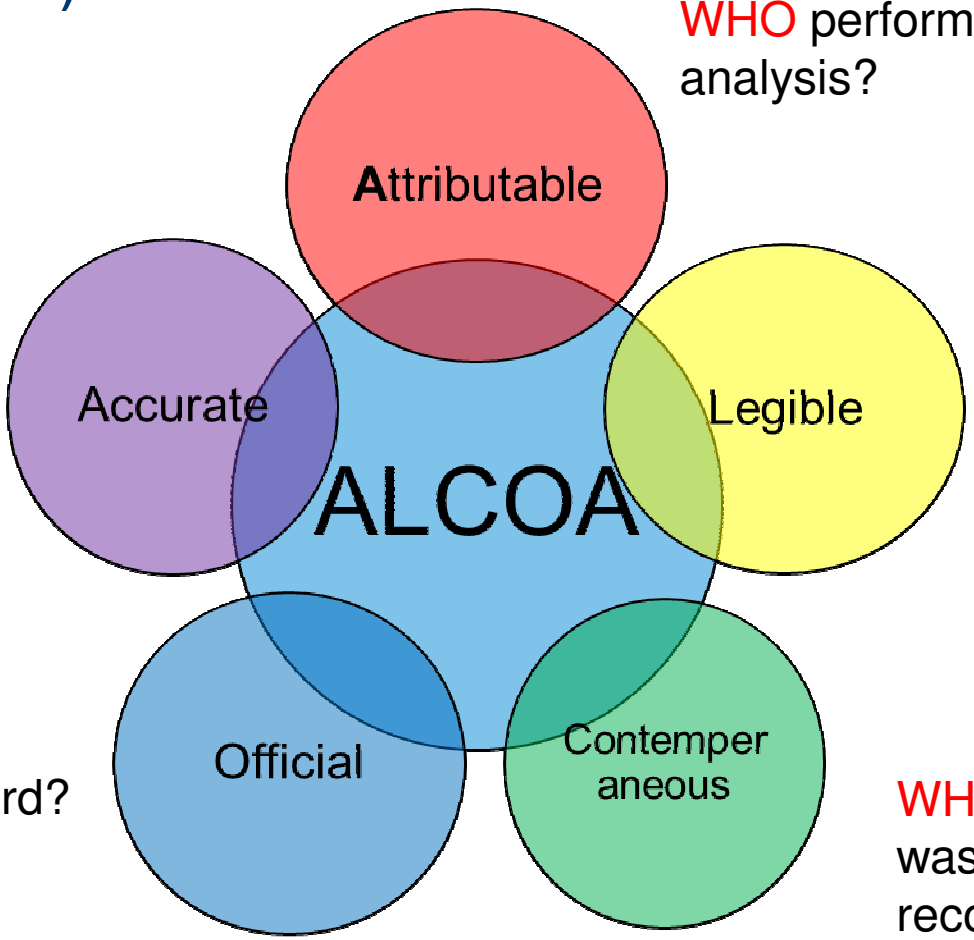
WIN AS ONE

Good Documentation Practice (GDP – ALCOA)

Good Documentation Practice (GDP – ALCOA)

WHO performed the analysis?

DOES the record accurately reflect the events that took place?



CAN the data be read and understood?

IS it the original record?
IS it the electronic record?
IS it Meta data?

WHEN and WHERE was the data created / recorded?

New Approach to Audit

New approach to Audit

- Focus - Potential for fraudulent activity within your quality systems.
- Assumptions:
  - Will assume fraudulent activity is taking place if they identify weaknesses in your quality systems.
  - "Guilty until proven innocent" approach to auditing!
  - "Data to good to be true!".

New approach to Audit

- Electronic data (Meta data) is - preferred choice for regulatory authorities as this is the original ("official") data.
- Meta data = data about data.
- Meta data is dynamic and can be queried / searched / trended.
- There is a much higher probability of identifying fraudulent activity within an organisation if Meta data is reviewed.
- Hard copy (Flat data – printed, pdf, photocopy) is no longer considered to be acceptable by regulatory authorities as this data is not complete and not original.
- If you state that paper is your original raw data in your internal procedures this will alert an auditor that you are probably not managing and reviewing electronic (meta) data.

New approach to audit - Flat data vs. Meta Data

Flat Data file → Printed Chrom OR Pdf Chrom OR Photo Chrom

- Analyst can reprocess data many time and chooses when to print, pdf or copy the final chromatogram / result from CDS.
- *DOES NOT PROVIDE FULL TRACEABILITY AS NO SUPPORTING DATA!*

Data file → Acq method + Proc method + Chrom + Audit trail

- *Provides full traceability as supporting data provides evidence how final chromatogram / result has been generated!*

New approach to Audit

- 5 key Data Integrity (DI) questions:
  - Is electronic data available?
  - Is electronic data reviewed?
  - Is meta data (audit trails) reviewed regularly?
  - Are there clear segregation of duties?
  - Has the system been validated for its intended use?

- The answers to the above questions will determine whether companies are in compliance with 21 CFR part 11 (Electronic records and signatures).

- Leave the Original Meta data in the CDS and review / approval electronically to avoid increased Data Integrity risk (the paperless lab).

WIN AS ONE

Data Integrity – Audit Preparation

Data Integrity – Audit Preparation

- Audit Strategy:
  - Starts with a specific result (or record).
  - Re-create the sequence of events that occurred at the time the result (or record) was generated using the electronic (meta) data.
- The auditor will want to know:
  - WHO performed the analysis?
  - WHAT equipment was used to perform the analysis?
  - WHEN the analysis was performed?
  - WHY the analysis was performed?
  - WHERE the electronic (meta) data is stored?
- Answers to the above may lead to more detailed questioning / inspection.

WIN AS ONE

Data Integrity – Risk Assessment

Data Integrity – Risk Assessment

USP <1058> (AIQ)	GAMP 5
A Basic equipment that does not generate results or need calibrated.	1 Instrumentation with firmware.
	2 Instrumentation with firmware and pre-defined programs.
B Equipment that generates results but does not need specialist calibration.	3 Instrumentation with non-configurable, commercial off-the-shelf software.
	4 Instrumentation with configurable, commercial off-the-shelf-software.
C Equipment that generates results and needs specialist calibration.	5 Instrumentation with bespoke software.

Increasing Data Integrity Risk

Data Integrity – Risk Assessment

Instrument type	USP<1058> categorisation	GAMP5 categorisation	Data integrity risk
Balance	B	2	LOW
pH meter	B	2	LOW
FT-IR	C	3	MEDIUM
UV	C	3	MEDIUM
HPLC	C	4	HIGH
GC	C	4	HIGH

- Do you have meta data for each system?
- Implement short and long term CAPA's

Can become high risk if older, stand-alone systems in use.

Data Integrity – Procedures / SOP's

Data Integrity – Procedures / SOP's

- The auditor will expect a suite of SOP's to be in place to support Data Integrity and minimise risk within your company.

- Examples of typical SOP's include:
  - IT policies.
  - System administration (CDS access, roles and privileges).
  - Data management and storage.
  - Data acquisition and processing.
  - Data review and approval.
  - Date archiving and back-up.
  - Anti-fraud monitoring.

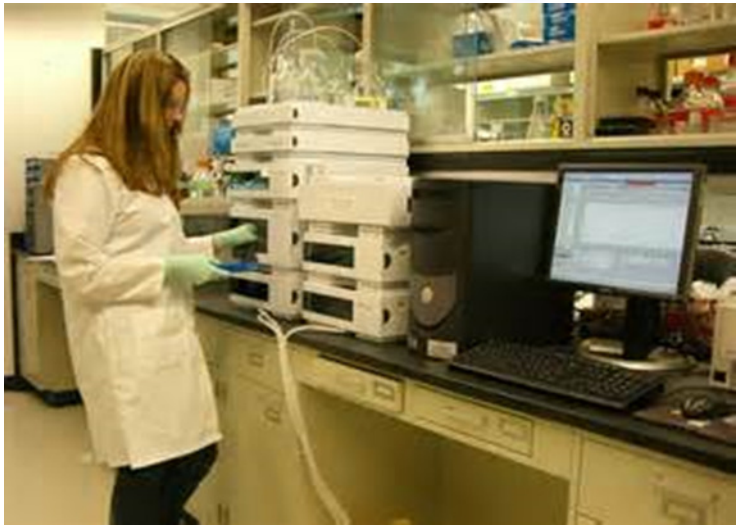
IT Infrastructure

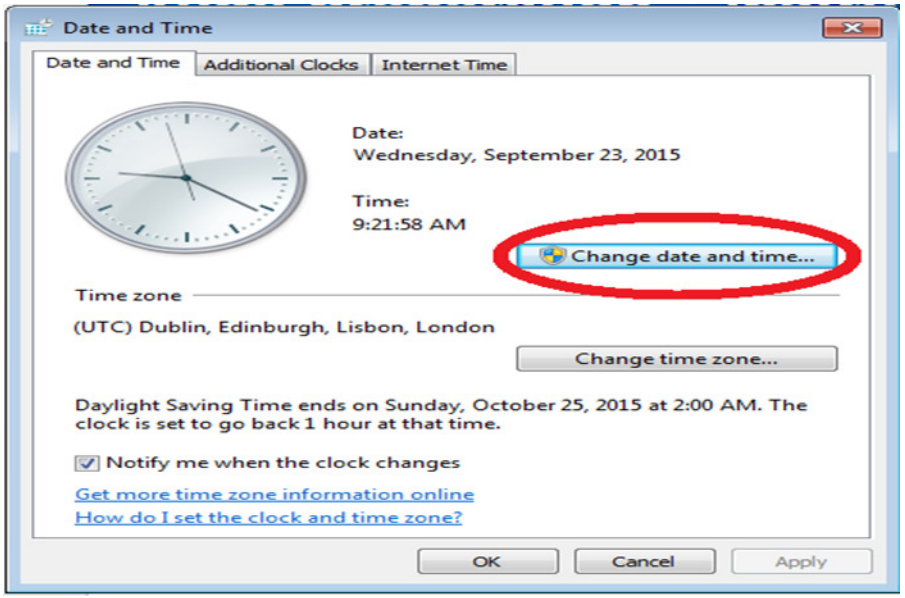
IT Infrastructure

- Server room:
  - The room is secure.
  - IT access only.
  - Tidy and in good working order.
  - Has back-up and disaster recovery procedures in place.
  - Date/time functionality of servers are correct.

IT Infrastructure

- The auditor will select a number of instrument controlling PC's within the lab and check:
  - Date/time functionality is correct.
  - Date/time cannot be changed by the lab personnel.





Confirm that date/time functionality on all PC's within the lab is locked down and can only be changed by IT personnel with Administration privileges.

WIN
AS
ONE

Administration

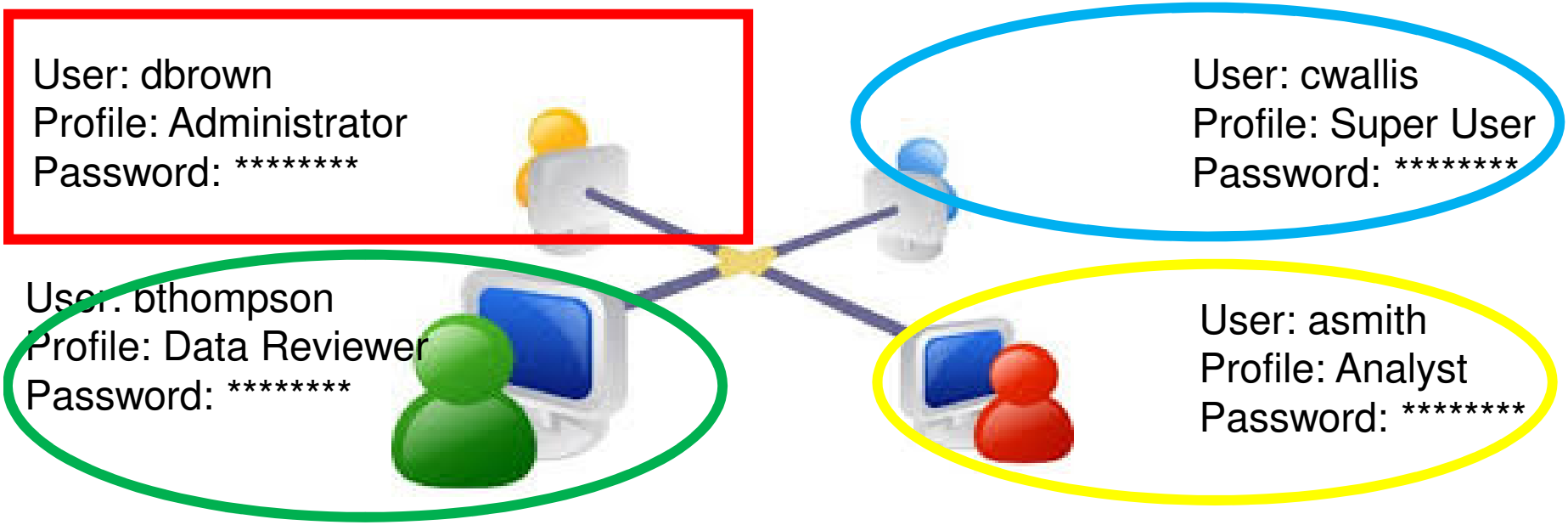
Administration

- The auditor will want to understand how access to the Chromatography Data System (CDS) is authorised and controlled.

- You will need to justify the access levels within the CDS and the user privileges at each level.

Administration

- Specific user profiles and passwords required to access instrument software and provide audit trail traceability.
- Administration control should be independent of Analytical function to eliminate conflict of interest.
- Clear segregation of duties with no overlap of privileges.



Administration

- Reinforce – DO NOT SHARE PASSWORDS.
- Password policies - changed on a regular basis to protect your profile.
- Password strength - mix of alpha numeric characters and have a high strength.
- User policies - need to log-off the CDS immediately after use to avoid profile potentially being used by other personnel to acquire, process or manipulate data.
- User profiles - set to auto-lock after a period of inactivity to protect the user profile and data within the CDS.

Administration

- The regulatory auditor will want to confirm that the Audit Trail functionality is switched ON within the CDS Admin console.

- The regulatory auditor may ask for Administration reports:
  - Active users
  - User privileges
  - Administration audit trail report

Administration

- Specific privileges within the user profile:

  - They will want assurance that data cannot be deleted by a user once acquired.

  - They will want to know if data can be moved to a different folder to potentially "hide" it. (e.g. trial injections)

Administration

- They will want to see that electronic data that has been processed must be saved before it can be submitted for review (or printed to hard copy).

Make sure you understand the privileges applied to each user profile and be prepared to justify to the regulatory auditor.

Data Management

Data Management

- The auditor will want to understand how data is managed within the CDS and check that users are following the internal procedure.

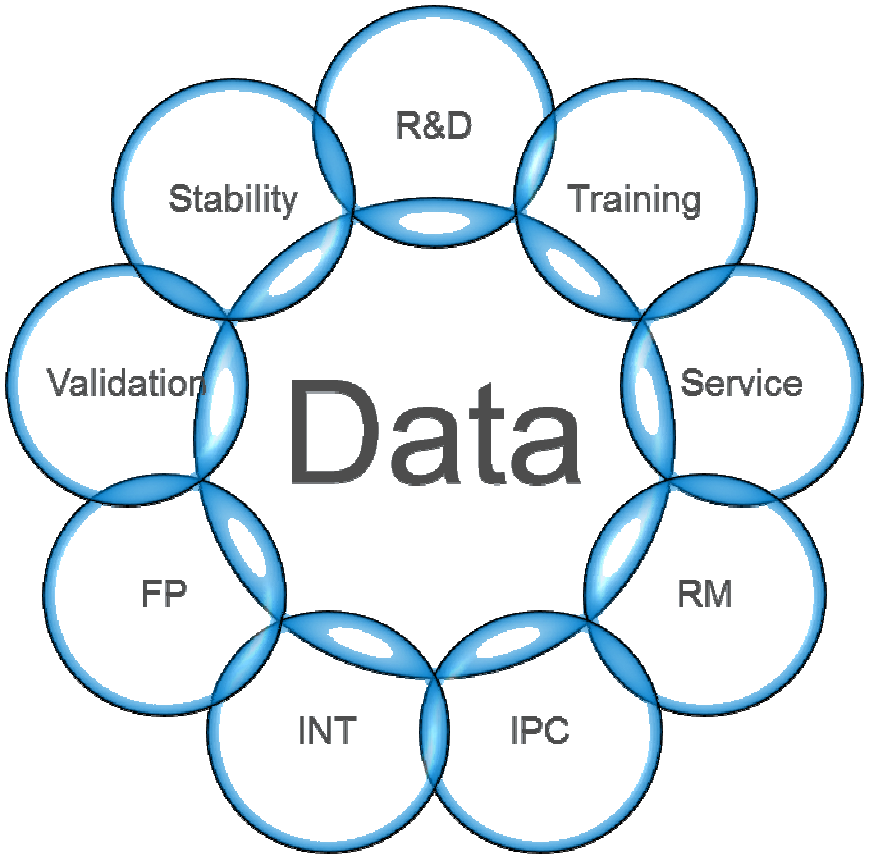
- Define a data management structure that segregates different types of data and enables easy retrieval during the audit.

- Segregate GMP release data is from Research / Development data if you have dual functionality within your organisation using the same CDS / Server.

Data Management

- Data structure - Consider what types of data you produce and decide how each type of data should be stored within the CDS.

Good data management - will give the auditor confidence that you have control over your electronic (meta) data and will increase retrieval speed during the audit.

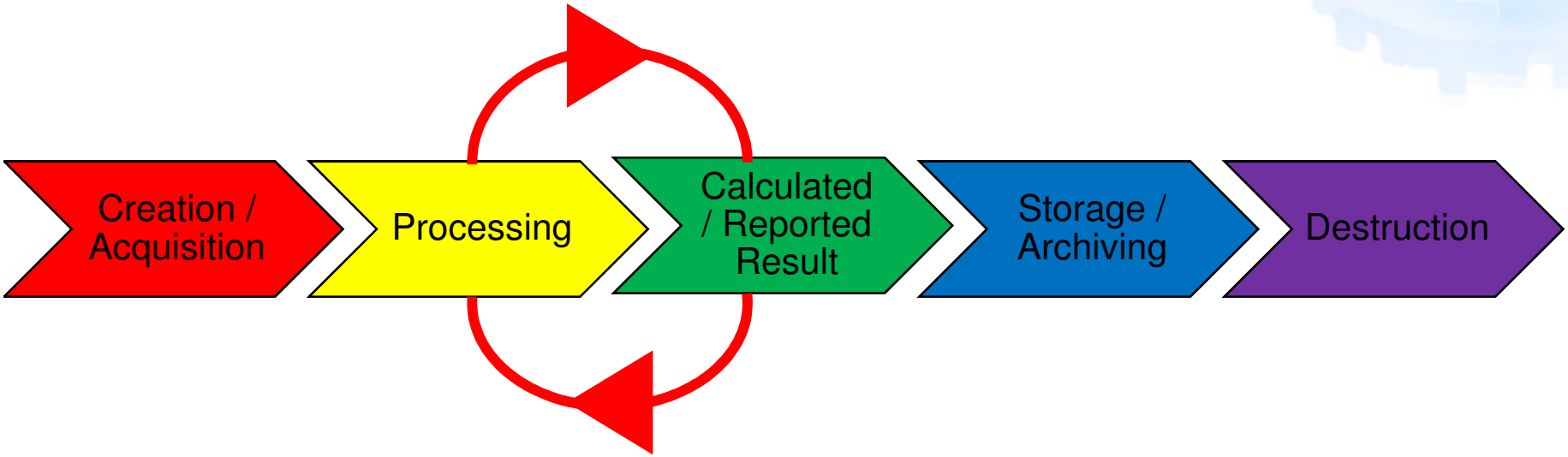


Data Management

- Periodic GMP data archiving – make sure that data archiving is defined in your procedure and performed regularly.
- This approach minimises the amount of “live” data that can be accessed by users and potentially reprocessed to change previously reported results.
- The users should not have access to archive folder(s) which adds an additional layer of protection to the electronic data.

Data Processing

Data Processing



- Data Processing Risks:
  - Main area where results can be manipulated by human intervention.
  - Target area for auditors.
  - Controlled by procedures, user access and locked methods.
  - Avoid multiple reprocessing (if possible)!

Data Processing

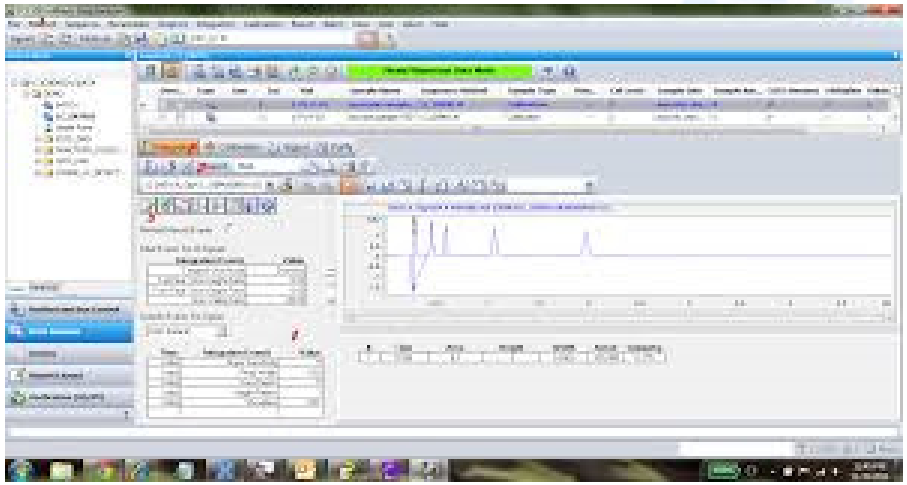
- All data processing should be performed within the CDS for system suitability and batch results wherever possible.

- Move away from using validated excel spreadsheets (no longer meta data).

- For commercial release testing the auditor will expect processing methods to be validated and locked by the administrator.

Data Processing

- Use pre-defined integration parameters wherever possible to avoid manual integration of multiple peaks.

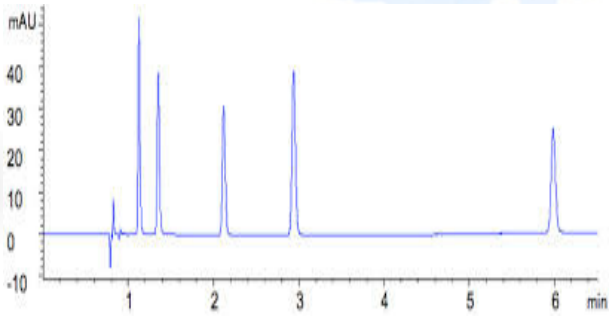


- Chromatography should be presented on an appropriate scale so that integration is clearly visible.

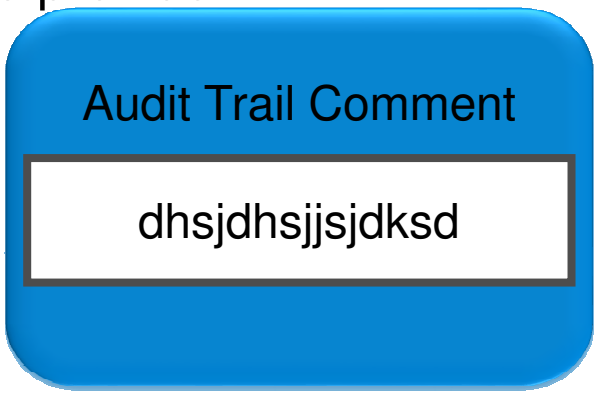
- Disable annotation tools within the CDS (electronic tippex!) which could be used to deliberately alter the appearance of the chromatograms.

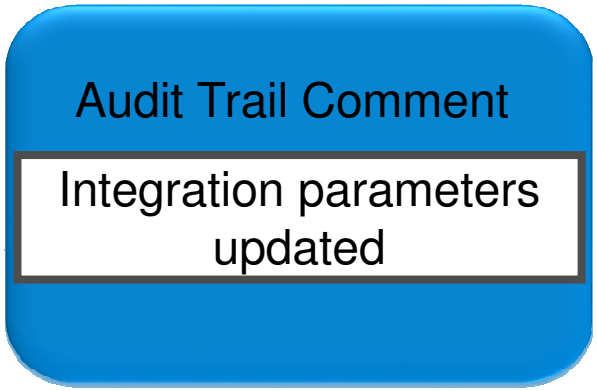
Data Processing

- Save all changes to individual chromatograms, sequences and processing methods before submitting for review.



- Ensure that accurate audit trail comments are entered into the CDS when prompted to provide traceability.





WIN AS ONE

Internal Data Review

Internal Data Review

- Parameters to check:
  - Analysis performed as per the monograph.
  - Sequence information correct.
  - Chromatography is typical.
  - SST acceptance criteria achieved.
  - NO “conditioning” or “test” injections using the sample (use a standard or control sample if specified by your procedures and monograph).
  - Correct integration (pay attention to MANUAL integration).
  - Chromatography appropriately scaled.

Data Review

- Individual results duplicate and meet specification.
- Check the sequence and individual injection audit trail - any atypical / suspect activity?
- Data processing:
  - Do the audit trail comments provide traceability?
  - Can the reprocessing be justified?
- Check electronic results within the CDS match results reported on hard copy chromatography or in LIMS / SAP systems.

External (Auditor) Data Review

External (Auditor) Data Review

- Auditor checklist:
  - Administration control.
  - Individual user profiles and passwords.
  - Clear segregation of duties within user profiles.
  - Restricted privileges for user (cant delete / over-write / move).
  - Audit trail functionality switched ON.
  - Date / time functionality locked by IT.
  - Lab Demo – User log-on (multiple), date / time locked, cant delete data.

External (Auditor) Data Review

- Auditor checklist:
  - Data recall – Electronic sequence / data file recall in lab using staff member. Data recall needs to be fast and efficient.
  - Data review – Chromatography scaling, integration and electronic results.
  - Audit trail review – looking for suspicious activity, justification of processing.
  - Training – assess staff competency with CDS in lab. Make sure staff are trained to interact with the auditor. Have a CDS super-user present during the lab inspection.
  - Query search –assurance that batch hasn't been analysed multiple times as part of an investigation.

External (Auditor) Data Review

- Auditor checklist:
  - Final electronic results in CDS match those reported on C of A.

FDA / MHRA inspectors have ben trained by Data Integrity and CDS experts!

They have detailed knowledge of your CDS and know where to find the meta data to identify if fraudulent activity has taken place!

Anti-Fraud Monitoring

Anti-Fraud Monitoring

- Expectation:
  - Anti-Fraud policies / procedures to be available.
  - Regular internal anti-fraud audits looking at different areas within your company / department.
  - Documented evidence of anti-fraud audits with associated CAPA's for audit findings.
  - QA / QP training for CDS to perform audit trail review before GMP batch release.

- Consider:
  - Having a Data Integrity / Anti-Fraud officer.
  - Perform spot-checks on lab operations outside the regular audit schedule.
  - Using video equipment to document physical activity.


Thank you
for your
attention
any
questions?

Appendix

Sources of Data Integrity Information

Sources of Data Integrity Information

MHRA
Regulating Medicines and Medical Devices

Data Integrity Guidance Document
www.gov.uk/government/publications/good-manufacturing-practice-data-integrity-definitions
Blog
www.mhrainspectorate.blog.gov.uk

FDA

Warning Letters
www.fda.gov/ICECI/EnforcementActions/WarningLetters
FDA Voice Blog
www.blogs.fda.gov

Health Canada

Inspection tracker
www.hc-sc.gc.ca/dhp-mps/pubs/compli-conform/tracker-suivi-eng.php

World Health Organization

Data Integrity Guidance Document
www.who.int/medicines/areas/quality_safety/quality_assurance/Guidance-on-good-data-management-practices_QAS15-624_16092015.pdf

Sources of Data Integrity Information

Eudra GMP Data Base
http://eudragmdp.ema.europa.eu/inspections/gmpc/searchGMPNonCompliance.do

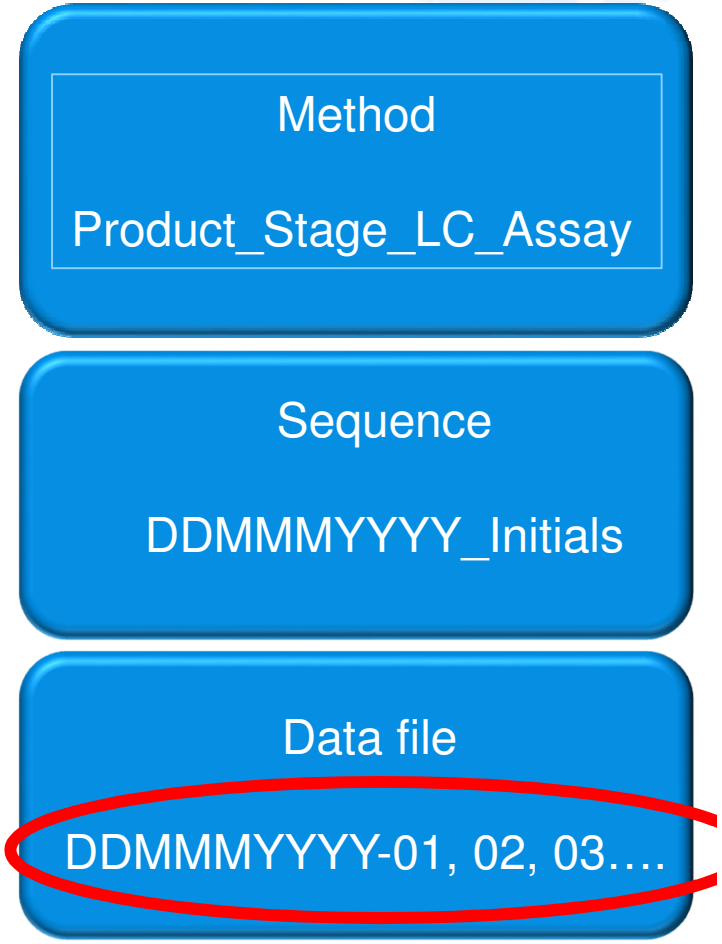
Data Integrity Specialist Interest Group (SIG) and Body of Knowledge tool (for members only).
iSpeak blog (free to access)
www.blog.ispe.org

Data Integrity discussion group.
Over 700 members.
Data integrity SME's regularly post information.

Data Acquisition

Data Acquisition

- Procedure requirements:
  - Clear instructions how to create an acquisition method from first principles.
  - Contain naming conventions for the methods, sequences and individual data files. This approach provides continuity between analysts and also helps with data retrieval.
  - Define the date format used by your company so there is no confusion between EU vs US format.



WIN AS ONE

Data Integrity – Audit Preparation

Data Integrity – Audit Preparation

- Research the background of the auditor(s) to gain knowledge of their experience and areas of expertise.
- Use available resources:
  - Existing Industry contacts
  - Internet searches
  - LinkedIn

WIN AS ONE

Data Integrity – Risk Assessment

Data Integrity – Risk Assessment

- Risk assess all lab areas prior to the audit to identify equipment that produce electronic data files.
- Categorise the equipment according to USP<1058> and GAMP5.
- Auditors will focus on instrumentation that falls under USP<1058> categories B and C and GAMP5 categories 3, 4 and 5.

Data Integrity – Risk Assessment

- Perform an internal Data Integrity audit on medium and high risk equipment.
- Does the equipment meet the requirements of 21 CFR part 11 (as yourself the 5 questions regarding electronic data)?
- Check that electronic data can only be accessed through the instrument software and not via the operating system.
- Identify gaps and implement short term corrective action before audit (if possible):
- Discuss longer term corrective actions with management team.