Agenda

- FDA inspection findings for data integrity issues – 40 minutes
- Top 5 Misconceptions About Data Integrity – 20 minutes
- Data Integrity Challenges and Solutions – 120 minutes
- How Can LIMS Help Ensure Data Integrity – 50 minutes
- Q & A – 10 minutes

FDA inspection findings for data integrity issues

21 CFR part 11 – Past, Present & Future

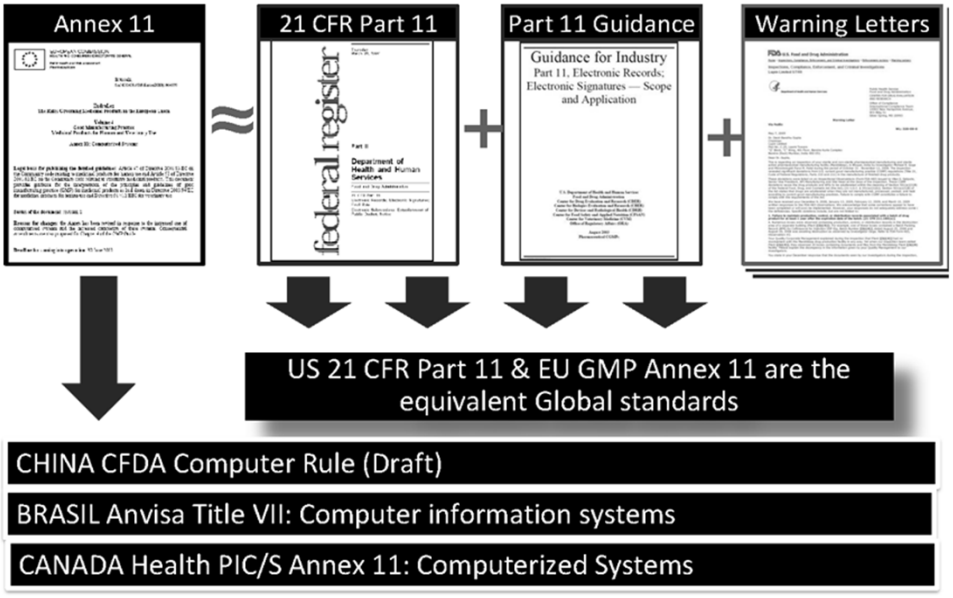
1997	**Part 11 Released**
1999-2003	Enforcement according to the letters of the rule
2003	New interpretation according to new guidance (Scope and Applications)
2003	Announcement of the new part 11
2003-2006	Enforcement stopped
2006-2010	Enforcement Starts again
2010-2014	Special Part 11 Inspection Program • Series of inspections with evaluation of industry's part 11 compliance and determine industry's interpretation of 21 CFR part 11 (2003 guidance) • Focus on critical items as found in previous inspections • Results to be used to determine next steps • Alternatives/considerations for next step – No change, New guidance, New part 11, Change inspection's focus and enforcement
On-going	**Focus on data integrity and security** **Data Integrity** is the assurance that data records are accurate, complete, intact and maintained within their original context, including their relationship to other data records. This applies to data recorded in electronic, paper formats or a hybrid of both. **Data Security** means that the data is restricted to authorized personnel and monitored through the system's software with its required log-on, security procedures, and audit trail. In addition, system software does not allow data manipulation with justification.

21 CFR part 11 Nowadays

Focus on data integrity and security

- **Data Integrity** is the assurance that data records are accurate, complete, intact and maintained within their original context, including their relationship to other data records. This applies to data recorded in electronic, paper formats or a hybrid of both (套用在電子記錄, 紙本記錄或兩者共存的記錄).
- **Data Security** means that the data is restricted to authorized personnel and monitored through the system's software with its required log-on, security procedures, and audit trail(需登錄管制, 安全程序及追溯稽核). In addition, system software does not allow data manipulation with justification(不允許無理由的操弄數據).

Global Compliance Standards



US FDA Inspection Trends

- FDA-483 Turbo citations
- cGMP Worming Letter issues

FDA Form 483

U.S. FOOD & DRUG ADMINISTRATION

FDA Form 483 Frequently Asked Questions

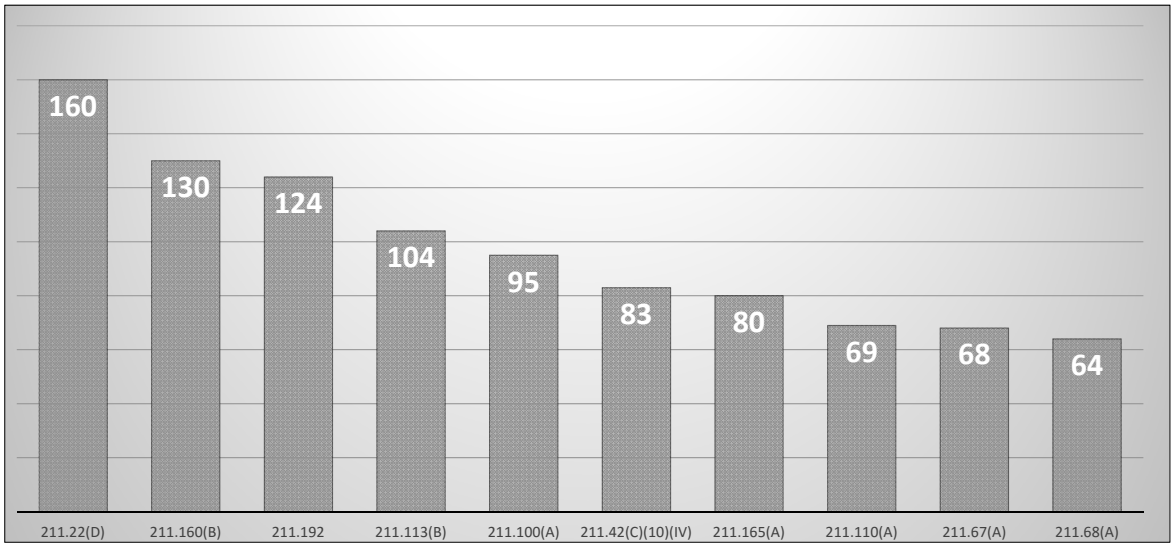
Q: When is an FDA Form 483 issued?

A: An FDA Form 483 is issued to firm management at the conclusion of an inspection when an investigator(s) has observed any conditions that in their judgement may constitute violations of the Food Drug and Cosmetic (FD&C) Act and related Acts. FDA investigators are trained to ensure that each observation noted on the FDA Form 483 is clear, specific and significant. Observations are made when in the investigator's judgement, conditions or practices observed would indicate that any food, drug, device or cosmetic has been adulterated or is being prepared, packed, or held under conditions whereby it may become adulterated or rendered injurious to health.

Q: What is the purpose of an FDA Form 483?

A: The FDA Form 483 notifies the company's management of objectionable conditions. At the conclusion of an inspection, the FDA Form 483 is presented and discussed with the company's senior management. Companies are encouraged to respond to the FDA Form 483 in writing with their corrective action plan and then implement that corrective action plan expeditiously.

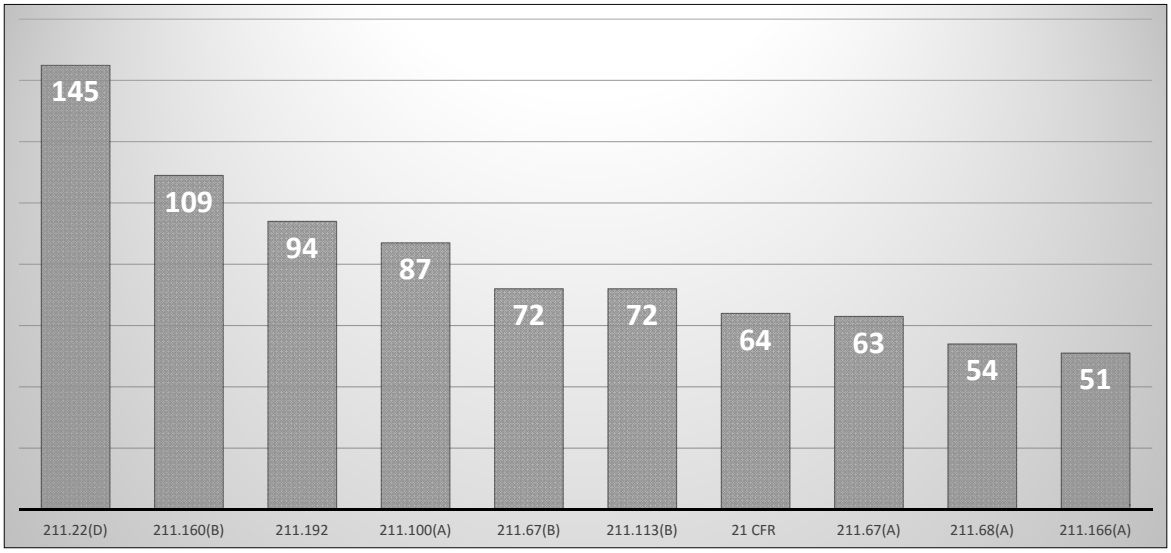
2015 Top 10 Cited Items



Descriptions of 2015 Top 5 Citations

211.22(d)	Procedures not in writing, fully followed
211.160(b)	Scientifically sound laboratory controls
211.192	Investigations of discrepancies, failures
211.113(b)	Procedures for sterile drug products
211.100(a)	Absence of Written Procedures

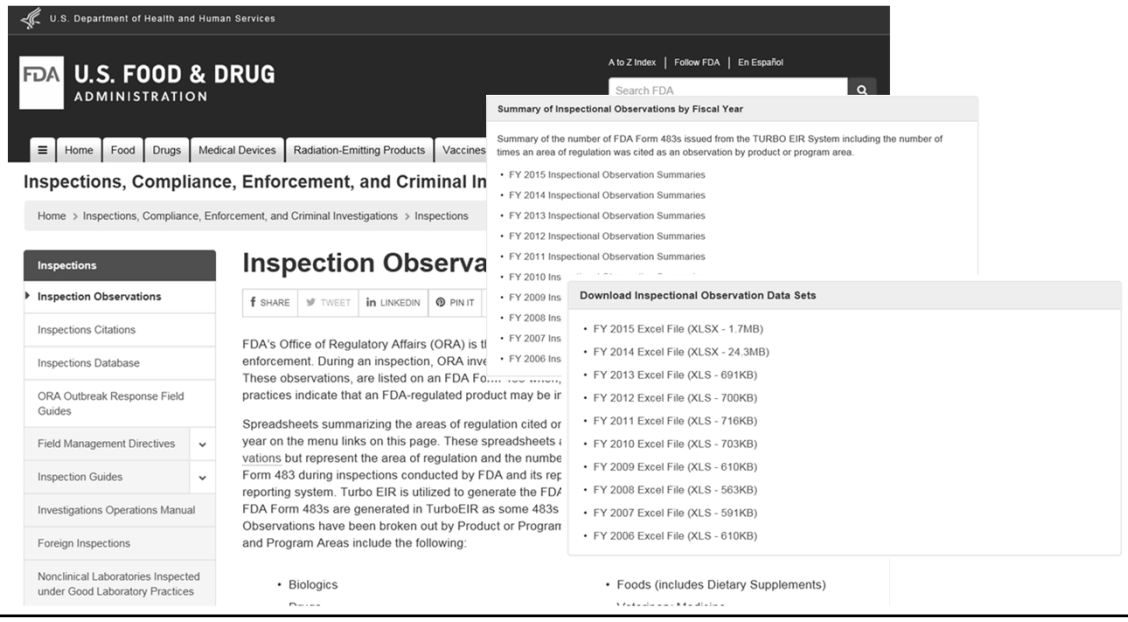
2014 Top 10 Cited Items



2011~2013 Top 10 Cited Items

2011	2012	2013
▪ 211.22(d)	▪ 211.22(d)	▪ 211.22(d)
▪ 211.100(a)	▪ 211.192	▪ 211.192
▪ 211.160(b)	▪ 211.100(a)	▪ 211.100(a)
▪ 211.192	▪ 211.160(b)	▪ 211.160(b)
▪ 211.25(a)	▪ 211.110(a)	▪ 211.67(b)
▪ 211.100(b)	▪ 211.67(b)	▪ 211.113(b)
▪ 211.67(b)	▪ 211.68(a)	▪ 211.67(a)
▪ 211.67(a)	▪ 211.25(a)	▪ 211.165(a)
▪ 211.165(a)	▪ 211.67(a)	▪ 211.110(a)
▪ 211.110(a)	▪ 211.100(b)	▪ 211.166(a)

FDA Web Site - www.fda.gov/ICECI/Inspections



Inspections Observations FY2015

Inspections_Observations_FY15 (final).xlsx - Excel

Center Name	Cite Id	Reference Number	Short Description	Long Description	Frequency
Drugs	1105	21 CFR 211.22(d)	Procedures not in writing, fully followed	The responsibilities and procedures applicable to the quality control unit are not [in writing] [fully followed]. Specifically, ***	160
Drugs	3603	21 CFR 211.160(b)	Scientifically sound laboratory controls	Laboratory controls do not include the establishment of scientifically sound and appropriate [specifications] [standards] [sampling plans] [test procedures] designed to assure that [components] [drug product containers] [closures] [in-process materials] [	130
Drugs	2027	21 CFR 211.192	Investigations of discrepancies, failures	There is a failure to thoroughly review [any unexplained discrepancy] [the failure of a batch or any of its components to meet any of its specifications] whether or not the batch has been already distributed. Specifically, ***	124
Drugs	1451	21 CFR 211.113(b)	Procedures for sterile drug products	Procedures designed to prevent microbiological contamination of drug products purporting to be sterile are not [established] [written] [followed]. Specifically, ***	104
Drugs	1361	21 CFR 211.100(a)	Absence of Written Procedures	There are no written procedures for production and process controls designed to assure that the drug products have the identity, strength, quality, and purity they purport or are represented to possess. Specifically, ***	95
Drugs	1434	21 CFR 211.42(c)(10)(iv)	Environmental Monitoring System	Aseptic processing areas are deficient regarding the system for monitoring environmental conditions. Specifically, ***	83
Drugs	1883	21 CFR 211.165(a)	Testing and release for distribution	Testing and release of drug product for distribution do not include appropriate laboratory determination of satisfactory conformance to the [final specifications] [identity and strength of each active ingredient] prior to release. Specifically, ***	80
Drugs	3585	21 CFR 211.110(a)	Control procedures to monitor and validate performance	Control procedures are not established which [monitor the output] [validate the performance] of those manufacturing processes that may be responsible for causing variability in the characteristics of in-process material and the drug product. Specifically	69
Drugs	1213	21 CFR 211.67(a)	Cleaning / Sanitizing / Maintenance	Equipment and utensils are not [cleaned] [maintained] [sanitized] at appropriate intervals to prevent [malfunctions] [contamination] that would alter the safety, identity, strength, quality or purity of the drug product. Specifically, ***	68
Drugs	1274	21 CFR 211.68(a)	Calibration/Inspection/Checking not done	Routine [calibration] [inspection] [checking] of [automatic] [mechanical] [electronic] equipment is not performed according to a written program designed to assure proper performance. Specifically, ***	64
Drugs	1914	21 CFR 211.166(a)	Lack of written stability program	There is no written testing program designed to assess the stability characteristics of drug products. Specifically, ***	63
Drugs	1435	21 CFR 211.42(c)(10)(v)	Cleaning System	Aseptic processing areas are deficient regarding the system for cleaning and disinfecting the [room] [equipment] to produce aseptic conditions. Specifically, ***	60
Drugs	1177	21 CFR 211.63	Equipment Design, Size and Location	Equipment used in the manufacture, processing, packing or holding of drug products is not [of appropriate design] [of adequate size] [suitably located] to facilitate operations for its [intended use] [cleaning and maintenance]. Specifically, ***	56
Drugs	2009	21 CFR 211.188	Prepared for each batch, include complete information	Batch production and control records [are not prepared for each batch of drug product produced] [do not include complete information relating to the production and control of each batch]. Specifically, ***	56
Drugs	1215	21 CFR 211.67(b)	Written procedures not established/followed	Written procedures are not [established] [followed] for the cleaning and maintenance of equipment, including utensils, used in the manufacture, processing, packing or holding of a drug product. Specifically, ***	53

Summary | Biologics | Bioresearch Monitoring | Devices | Drugs | Foods | Human Tissu ...

READY

FDA Warning Letter

FDA U.S. FOOD & DRUG ADMINISTRATION

FDA Basics Questions

What is a Warning Letter?

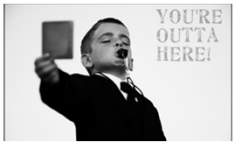
When FDA finds that a manufacturer has significantly violated FDA regulations, FDA notifies the manufacturer. This notification is often in the form of a Warning Letter.

The Warning Letter identifies the violation, such as poor manufacturing practices, problems with claims for what a product can do, or incorrect directions for use. The letter also makes clear that the company must correct the problem and provides directions and a timeframe for the company to inform FDA of its plans for correction. FDA then checks to ensure that the company's corrections are adequate.

FDA Warning Letter

- FDA Form 483 is referred to as “Notice of Inspectional Observations.”
- The 483 is issued by the FDA field investigator after an on-site inspection.
- It lists deficiencies in your quality system.
- The observations are based on the inspector’s interpretation to the regulations as they relate to your operational GMP quality system.
- The field inspector will submit finalized 483 to his/her superiors; based on **the severity of the findings**, an **FDA Warning Letter** may be issued to your firm.**(發現嚴重違規項目, 警告信)**

A Sample of Warning Letter



Emcure Pharmaceuticals Limited 3/3/16

Department of Health and Human Services

Public Health Service
Food and Drug Administration
Silver Spring, MD 20993

Warning Letter

VIA UPS

WL: 320-16-08

March 3, 2016

Mr. Satish Mehta
Chief Executive Officer
Emcure Pharmaceuticals Ltd.,
Plot No. P-1, IT BT Park Phase II, MIDC, Hinjwadi
Pune 411 057, Maharashtra
India

Dear Mr. Mehta:

From January 27 to February 4, 2015, the U.S. Food and Drug Administration (FDA) inspected your pharmaceutical manufacturing facility, Emcure Pharmaceuticals Limited, located at Plot No. P-1, IT BT Park Phase II, MIDC, Hinjwadi, Pune 411 057,

Within 15 working days of receipt of this letter, please notify this office in writing of the specific steps that you have taken to correct and prevent the recurrence of violations. In addition to the specific requests noted above, supporting documentation should include your third party assessment of the following.

1. A comprehensive evaluation of the extent of the inaccuracy of your recorded and reported data. Include a detailed action plan to fully investigate the extent of your deficient documentation and data management practices.

2. A risk assessment of the potential effects of observed failures on the quality of your drug products, including the effects of deficient documentation and data management practices, aseptic processing breaches, and inadequate environmental monitoring program. Determine the effects of your failures on the quality of drug products released for distribution and the data supporting all associated submissions.

3. A management strategy for your firm that includes the details of your corrective action and preventive action plan. Describe the actions you will take, such as contacting your customers, recalling drugs, conducting additional testing and/or adding lots to your stability programs, or other steps to assure the quality of your drugs manufactured under the deficient conditions discussed above. Also indicate measures you will take, such as revising procedures, implementing new controls, training or re-training personnel, or other actions to prevent the recurrence of CGMP violations, including breaches of data integrity.

Direct Costs of a Warning Letter

- **Corrective Action 矯正措施**

  Companies who receive a warning letter incur some amount of corrective action costs in order to address the FDA's concerns. Some companies also implement a corrective action team.

- **Consultants 顧問費用**

  In order to properly implement the corrective action plan and perhaps team, a company may need to hire additional consultants to help respond and identify problems.

- **Quality Systems Improvement Initiatives 啟動品管系統改善**

  As part of the corrective actions, companies also implement and spend time and money establishing a QSII.

- **Fines 罰款**

  Fines are unique to each case and can be quite significant.

- **Plant Closing/Production Halt 關廠/停工**

  After spending much time and money as a result of the warning letter, many companies who have been unsuccessful in remediating issues are forced to halt product manufacturing or even close their facilities.

Indirect Costs of an FDA Warning Letter

- A damaged public reputation 商譽受損
- Competitor opportunity 對手商機
- Severed contracts 難接訂單
- Angry stockholders 股東責難
- Distractions from growth 阻礙成長

Warning Letters Issued in 2015

Totally issued **50** drug GMP warning letters

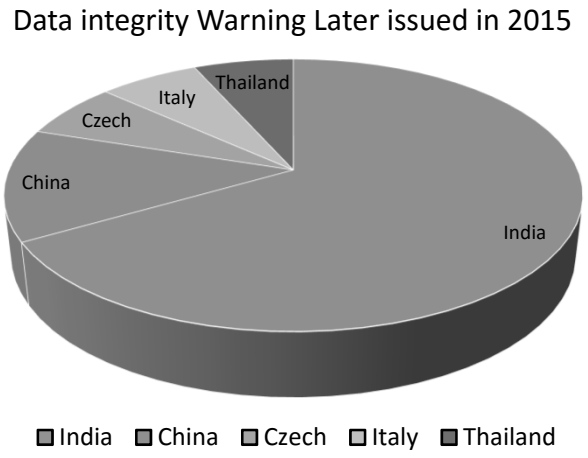
- **31** in US

  To compounding pharmacies, all located in the US. This continues FDA's extraordinary inspection and enforcement focus on this industry segment which began in 2014

- **19** outside US

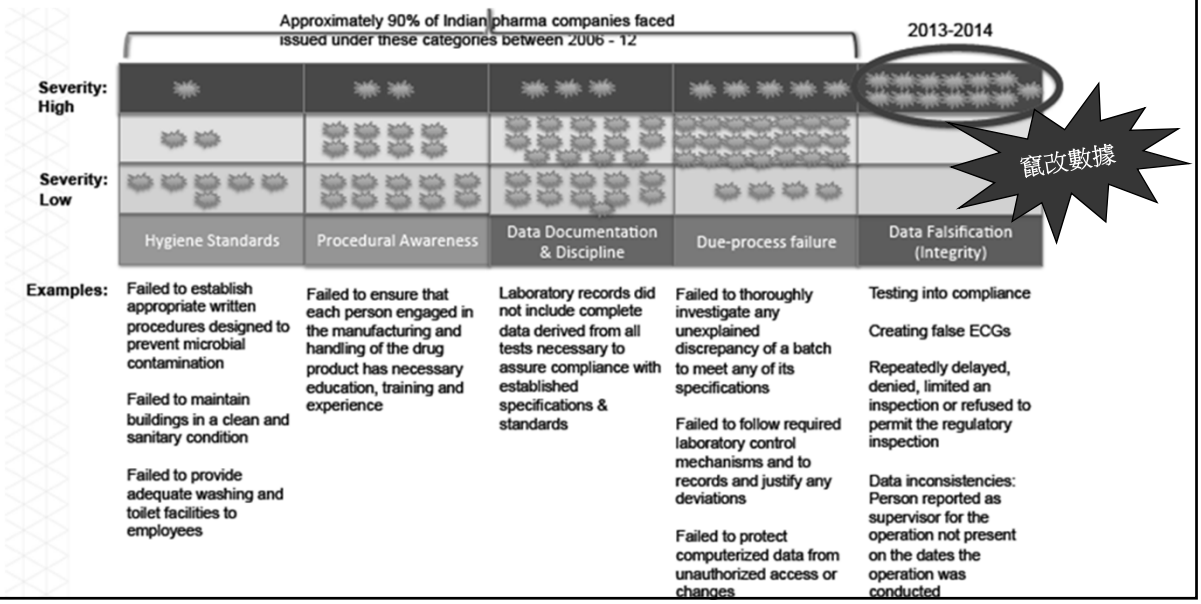
  Fifteen (15) of those included **data integrity** associated deficiencies

Warning Letters of Data Integrity in 2015



India	**10**
China	**2**
Czech	**1**
Italy	**1**
Thailand	**1**

India has a system problem



FDA 2015.2.27 發給印度某藥廠的警告信

- Failure to prevent unauthorized access or changes to data and to provide adequate controls to prevent omission of data. The inadequate controls over access to your data raise questions about the authenticity and reliability of your data and the quality of the APIs you produce. Specifically,There was no written explanation for deletion events observed on audit trials for your standalone HPLC units. Your SOPs did not include instructions for the retention of electronic raw data. In response to this letter, provide your procedure describing requirements to maintain complete data.
  a) Your firm did not have proper controls in place to prevent the unauthorized manipulation of your laboratory's raw electronic data. Your HPLC computer software lacked active audit trail functions to record changes to analytical methods, including information on original methodology, the identity of the person making the change, and the date of the change. In addition, your laboratory systems did not have access controls to prevent deletion or alteration of raw data. During the inspection, your analysts demonstrated that they were given inappropriate user permissions to delete HPLC data files.
  b) Moreover, the gas chromatograph (GC) computer software lacked password protection allowing uncontrolled full access to all employees. Your response states that you commit to upgrading your HPLC systems to have audit trails and your GC system to have password protection by July 31, 2014. However, your response lacks sufficient detail of the systems and controls you will implement. Simply turning on audit trail functions is inadequate. In addition, you failed to review historical data to ensure the quality of your products distributed to the US market.

  In response to this letter, provide specific details about the comprehensive controls in place to ensure the integrity of electronic raw data generated by all computerized systems during the manufacture and testing of your drugs. Your response should demonstrate an understanding of your processes and the appropriate controls needed for each stage of manufacturing and testing that generates electronic raw data. Your response should also describe the controls and procedures you will implement to retain and archive the raw data you generate.

FDA 2015.9.28 發給印度某藥廠的警告信

- During our March 18-21, 2014 inspection of your pharmaceutical manufacturing facility, India, an investigator from the U.S. Food and Drug Administration (FDA) identified significant deviations from current good manufacturing practice (CGMP) for the manufacture of active pharmaceutical ingredients (APIs). These deviations cause your APIs to be adulterated within the meaning of Section 501(a)(2)(B) of the Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. 351(a)(2)(B). The methods used in, or the facilities or controls used for, their manufacture, processing, packing, or holding do not conform to, or are not operated or administered in conformity with, CGMP.

1. Failure to document production and analytical testing activities at the time they are performed.
2. Failure to prevent unauthorized access or changes to data and to provide adequate controls to prevent omission of data.
3. Failure to maintain complete data derived from all testing, and to ensure compliance with established specifications and standards.
4. Failure to properly maintain buildings and facilities used in the manufacture of intermediates and APIs in a clean condition.

FDA 2015.4.6 發給中國某藥廠的警告信

1. Failure to prevent unauthorized access or changes to data and to provide adequate controls to prevent omission of data.

You lacked controls to prevent the unauthorized manipulation of your laboratory's electronic raw data. Specifically, your infrared (IR) spectrometer did not have access controls to prevent deletion or alteration of raw data. Furthermore, the computer software for this equipment lacked active audit trail functions to record changes to data, including information on original results, the identity of the person making the change, and the date of the change. Audit trails that capture such critical data about the quality of your batch production should be reviewed as part of the batch review and release process.

2. Failure of your quality unit to ensure that materials are appropriately tested and the results are reported.

The inspection documented that an analyst at your firm failed to perform the IR identity test for all lots of **(b)(4)**, API, as part of your quality control release. Instead, the analyst at your firm altered the file name in the spectrophotometer containing the sample identification information for **(b)(4)** API lot # **(b)(4)**, tested on April 2, 2014, to support the release of two previously manufactured lots, # **(b)(4)** and **(b)(4)**.

Remediation Cost and Revenue Loss – Case 1

Major global manufacturer received WL in early 2012 for a US plant, highlighting GMP and testing issues.

This led to reduced output and the eventual closure of the facility for 9 months. The WL was closed out two years later. **(關廠)**

- Remediation Cost: **$64 million**
- Lost Revenue: **$35 million**
- Opportunity Costs: **$9 million**

Remediation Cost and Revenue Loss – Case 2

Large India-based manufacturer received WL for India facility in late 2015.

Previously FDA approved innovator drug rescinded**(撤照)**, generic production forced to move. Site reinspection not likely until Q2 2017.

- Remediation Cost: **$113-133 million**
- Lost Revenue: **$25-$45 million**
- Opportunity Costs: **$13.5 million**

Remediation Cost and Revenue Loss – Case 3

Global manufacturer received WL and import ban for 2 facilities on Jan 2015 and Mar 2015. **(**禁止進口**)**

Currently in remediation.

- Remediation Cost: **$148-178 million**
- Lost Revenue: **$40-70 million**
- Opportunity Costs: **$26 million**

Remediation Cost and Revenue Loss – Case 4

Large India-based manufacturer received FDA Import alert in early 2013, followed by MHRA recall of multiple products. 2nd facility import alert in late 2013, expanded to all company APIs. All US products recalled early 2015. **(**延燒到所有**API**並回收所有在美國的產品**)**

MHRA closed out late 2015, with FDA close out expected Q2 2016.

- Remediation Cost: **$911 million**
- Lost Revenue: **$100 million**
- Opportunity Costs: **$51 million**

GMP Regulatory Requirements for Data Integrity

- Instruments must be qualified and fit for purpose [211.160(b), 211.63]
- Software must be validated [211.63]
- Any calculations used must be verified [211.68(b)]
- Data generated in an analysis must be backed up [211.68(b)]
- Reagents and reference solutions are prepared correctly with appropriate records [211.194(c)]
- Methods used must be documented and approved [211.60(a)]
- Methods must be verified under actual conditions of use [211.19r(a)(2)]
- Data generated and transformed must meet the criterion of scientific soundness [211.60(a)]
- Test data must be accurate and complete and follow procedures [211.194(a)]
- Data and the reportable value must be checked by a second individual to ensure accuracy, completeness and conformance with procedures [211.194(a)(8)]

FDA inspection findings for data integrity issues

- Failure to **prevent unauthorized access** by allowing **shared user accounts and passwords** and lack of **role-based security**
- Failure to **maintain complete data** derived from all laboratory tests conducted
- Failure to **investigate** and document **out-of-specification results**
- Failure to **prevent** the practices of product sample **retesting without investigation**

Top 5 Misconceptions About Data Integrity

Reference to Foundational Elements of Data Integrity

Misconception 1

- **Belief** that data integrity problems are **limited to fraud or falsification** **相信** data integrity **問題只針對欺騙或造假**
  - ➢Data Integrity also includes
    - Employee errors 錯誤
    - Mistakes 失誤
    - Omissions 疏失
    - Transcription errors (資料)傳遞錯誤
- Takeaway
  - **Management** is responsible to **ensure that all data is accurate** 確定所有資料都正確. They have a legal and moral obligation to ensure controls are in place to detect and prevent data integrity issues.

Misconception 2

- **Belief** that you **can trust employees** to follow policies and procedures

  相信你**可信任(你的)部屬**會遵照規範和程序

  - Sometimes employees do not follow procedures because the procedures are not clear or they (the employees) were not appropriately trained
  - Recent Health Authority inspections clearly demonstrate that employees sometimes do not following procedures and in some cases, deliberate falsification of data was uncovered. Management was not aware this was happening in their own facility.
  - What are the reason?
- Takeaway
  - **Management must have systems in place (**務必已在現場設定管理系統**)** to ensure that they (the employees) are following policies and procedures.

Misconception 3

- **Belief** that data integrity issues are **not likely to happen at your company**

  相信 data integrity issues 不大可能會發生在你公司

  - Inspections clearly demonstrate this is not true. Outcomes of many foreign inspections have been FDA Warning Letters, Notice of Concerns, import bans to both U.S. and EU and product seizures.
  - Recently, FDA filed criminal changes and prosecuted individuals for lying to investigators and impeding an investigation.
- Takeaway
  - Management should not be surprised by the serious nature of data integrity issues.
  - **The consequences** of not detecting and preventing data integrity issues can possibly **lead criminal prosecution and in one case – bankruptcy.**

    未偵測和避免的 **data integrity issues** 很可能導致違法指控**,** 最終破產

Misconception 4

- **Belief** that **employee error**, when found, **is the root cause** of data integrity issues, and that the solution is to retrain employees

  相信找到的**員工錯誤是** data integrity issues 的**根源**, 解決方式就是再教育員工
  - Human error is a symptom of a larger issue
  - It is NEVER the root cause
  - Simply retaining or even firing an employee is not an acceptable action
- Takeaway
  - **Management** is responsible and required to look further **to understand why the error occurred 真正了解為何錯誤發生**; example
    - Was there a procedure available?
    - Was the procedure followed?
    - Is the procedure adequate?
    - Many more questions to ask

Misconception 5

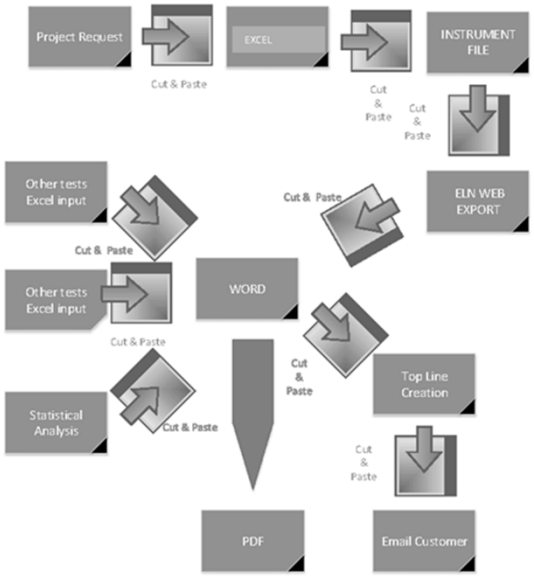
- **Belief** that recent activities in data integrity and enforcement in **data integrity is something new**

  相信近期 data integrity 的活動及要求是新的規範
  - Not new – data integrity and its enforcement have been around for decades
  - The single most important issue for FDA and other Health Authorities
- Takeaway
  - Why are we seeing more data integrity issues?
    - **Increase visibility 增加可見度** in the press and social media
    - Increase in inspections with a **focus on data integrity 聚焦 data integrity (Core objective of FDA) FDA 核心目標**
    - **More aggressive enforcement actions 更多積極要求行動** (Warning Letters, import bans, prosecutions, etc.)

The more they find
The more they look

Data Integrity Challenges
and
Solutions

Data Integrity Nightmare – Copy/Paste Madness



Contemporary Audit Approach

Assume fraudulent activity is taking place
if they identify weaknesses in your quality systems

Data is
too good to be true

Guilty until
proven innocent
(完成式)

Popular found issues

- No user specific passwords for instrument systems.
- Users have full access.
- Ability to change / delete electronic raw data.
- Failure to maintain complete data.
- No audit trail.
- Data not documented in real-time.
- Results recorded on unofficial documents.

Data Integrity Challenges

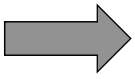
What is Data Integrity?

Data Integrity and Compliance With CGMP Guidance for Industry

For the purposes of this guidance, data integrity refers to the **completeness(**完整**)**, **consistency(**一致**)**, and **accuracy(**正確**)** of data.

Complete, consistent, and accurate data should be

- **attributable**
- **legible**
- **contemporaneously**
- **original /true copy**
- **accurate**



ALCOA

ALCOA

- In 2010, S.W. Woollen used the acronym ALCOA to describe attributes necessary to achieve Data Integrity.
- In 2010, ALCOA+ was introduced when the EMA(European Medicines Agency) published “Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials”

Data Integrity – Attributable 可歸屬

Who

performed the action?

Attributable data must be linked back to the specific individual who is responsible for observing and recording the data.

Attributable Data

Attributable – on Paper

Identify Verification and Authorization

- Identify should be verified
- Individual's name, initials and signatures should be documented
- Authorization to sign shall be detailed in SOPs and granted after training

Attributable – on Paper

Original Data Capture

- Data should be recorded directly, promptly, and legibly in indelible ink
- Data should be signed or initialled by the person entering the data
- Data should be date on the date of entry

Attributable – on Paper

Changes to Data

- Data changes recorded such as to not obscure the original entry.
- Reason for change shall be indicated
- Data shall be signed or initialled by the person correcting the data
- Data shall be dated on the date of change

Attributable – eRrecords

Identify Verification and Authorization

- Identify should be verified
- Individual's name, initials and signatures should be documented
- Assignment of Unique Electronic User ID(public name) with associated private password
- Affidavit stating e-Signature equivalent to handwritten signature
- Authorization to sign shall be detailed in SOPs and granted after training

Attributable – eRrecords

Original Data Capture

- Individual shall be identified at time of direct data input
- Audit trail shall capture detail around what actions were performed

Attributable – eRrecords

Changes to Data

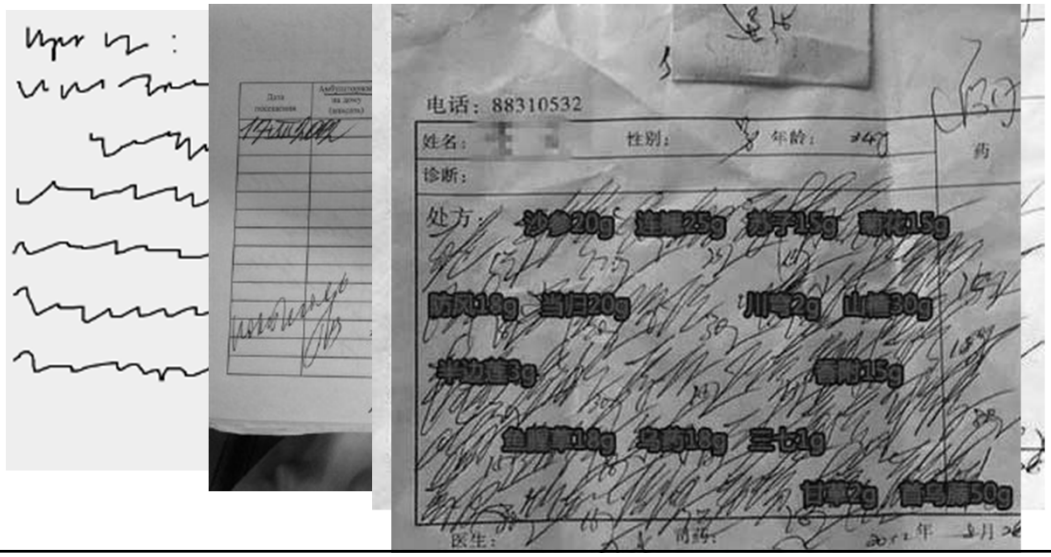
- The responsible individual making the change shall be permanently tied to record

Data Integrity – Legible 清晰可辨

Do you understand what is captured?

Legible data is clear, concise, permanent and readable.
Changes to legible data must not hide or obscure the original record

Legible Data - 1



Legible Data - 2

Legible Data - 3

GRAND CENTRAL STATION

GRAND CENTRAL STATION

Grand Central Station

Grand Central Station

Grand Central

Grand Central

Legible – Original Data

Original Data

The Original Value is

- **0.1502**

The Metadata is

- **grams**
- **David Lai**
- **01Aug2016 17:02:35**

How to record this data clear, concise, permanent and readable?

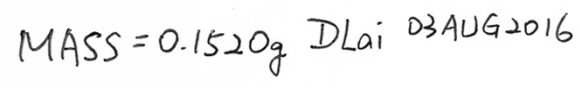
Legible Expectations

- Show the original Values and its metadata
- It is clear, readable and concise.
- It is also permanent. (e.g. indelible in used)
- Electronic Data must be in human readable format.

Legible Data – Paper V.S. eRecords

Show the original Values and its metadata

It is clear, readable and concise.



Date	Time	User	Value	Units	Reason
10-Aug-16	10:01:05	David Lai	0.1520	grams	Data Entry

It is also permanent. (e.g. indelible in used)

Electronic Data must be in human readable format.

Changes to Legible Data

- Maintains the original values and its metadata, does not obscure it!
- Changes and reason for change are clear, readable and concise.
- Changes are also permanent. (e.g. indelible ink used, not stored in RAM)
- Changes to Electronic Data must be in human readable format.

Changes to Legible Data – Paper V.S. eRecords

Maintains the original values and its metadata, does not obscure it!

Changes and reason for change are clear, readable and concise.

MASS = ~~0.1520g~~ DLai 03AUG2016

0.1502g transposed digits DLai 03AUG2016

Date	Time	User	Value	Units	Reason
10-Aug-16	10:01:05	David Lai	0.1520	grams	Data Entry
10-Aug-16	10:15:35	David Lai	0.1502	grams	Transposed Digits

Changes to Electronic Data must be in human readable format.

Changes are also permanent. (e.g. indelible ink used, not stored in RAM)

Data Integrity – Contemporaneous 即時記錄

Contemporaneous data must include the date and time of its measurement or action

Contemporaneous – Original Data

- Provide evidence of when data was observed and/or documented
- Typically captured in terms of date and time
- Time must be accurate
- Time should be linked to a Time Standard (e.g., NIST Time)
- Date and Time should be recorded in a unified predetermined format (e.g., DD MMMYY, HH:MM:SS, Military vs 12 Hour Clock, time zone, UTC,ect)

Contemporaneous – Paper Records

- Access to clocks are necessary for recording events.
- Clocks should be linked electronically to a centralized Time server or calibrated to a Time Standard that then should be periodical reviewed to secure accuracy.

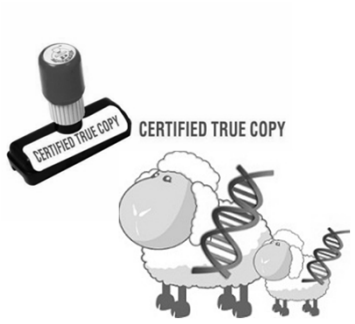
Issues to Consider

- Difficult to prevent and/or detect back-dating.
- Verifying contemporaneous data may require a witness.

Contemporaneous – Electronic Records

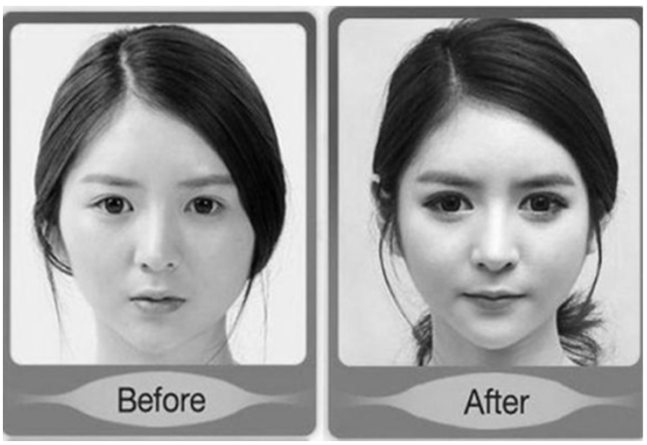
- Must use of secure, computer-generated, time-stamped audit trails.
- Audit trails should capture
  - Operator entries and actions that create, modify or delete electronic records.
  - Ensure audit trail functionality is turned on, has adequate space and is not purged.
  - Be selective with regards to audit trail content focus on critical data to create, modify and delete data
- Systems, servers and workstations should be linked to a centralized Time Server.
- Software should pull time from workstation or server electronic clocks.
- Electronic clocks should be secured on both workstations and servers such that they cannot be changed by users; Limit access to time controls only to administrators.

Data Integrity – Original 原始資料



Original data must be the original record or a certified true copy.

Data Integrity - Original



Data Integrity - Original

- Raw Data
  - Original records and documentation, retained in the format in which they were originally generated or as a “true copy”.
  - Simple electronic systems that do not store data and provide only printed data output, that printout constitutes the raw data.
- Differences between Dynamic and Static Files
  - Static files – e.g. paper, printed chromatogram, draft report
  - Dynamic files – e.g. electronic chromatogram
- True Copy
  - True Copy must include all metadata files
  - Snapshots are not whole story

Original - Expectations

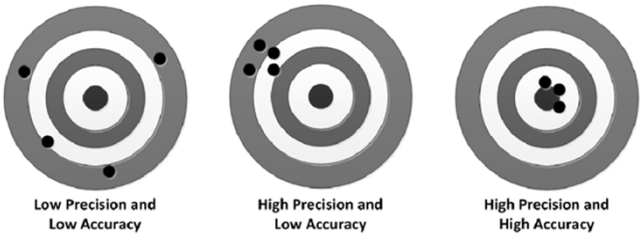
- Original records and true copies must preserve the following throughout the data’s lifecycle:
  - Accuracy - Correctness?
  - Completeness - Is it all there?
  - Content - Not obscured, available and readable.
  - Meaning of the record – doesn’t change
- Dynamic files should be maintained to enable filtering for complete inspection of data, not just snapshot.

Original - Expectations

- Good data management is necessary
  - Process controls around how data is created, modified and reported.
  - Data Backup and Restoration Practices to ensure data is not damaged or lost.
  - True Copy Verification Practices should be in place and documented.
- System testing should include confirmation that data and metadata can be backed up and recovered.

Data Integrity – Accurate 正確數據

Does your data show accuracy or just precision?



Accurate data is correct throughout the system's lifecycle. It indicates the same value and its correct meaning.

Data Integrity – Accurate

More accurate explanation is

No errors or editing
performed without documented amendments.

211.22(a) There shall be a quality control unit that shall have the responsibility and authority to approve or reject all components, drug product containers, closures, in-process materials, packaging material, labeling, and drug products, and the authority to review production records to assure that no errors have occurred or, if errors have occurred, that they have been fully investigated. …

Accurate - Expectations

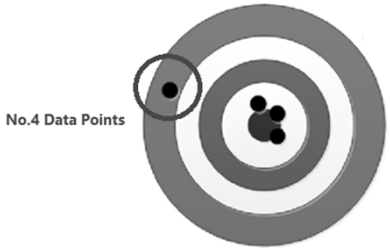
- Is your data correct? How do you know?
  - **Perform Testing** to ensure you are getting accurate data **during system use**.
  - **Verify Interfaces are tested** to ensure all the appropriate data is being received.
  - Accurate data should only be transferred from **calibrated/qualified systems and/or instruments.**
- Correctness includes the meaning of the record

ALCOA and ALCOA Plus Relationships

Completes Data Integrity by tying it all together

Data Integrity - Complete

Do you have all your Data?



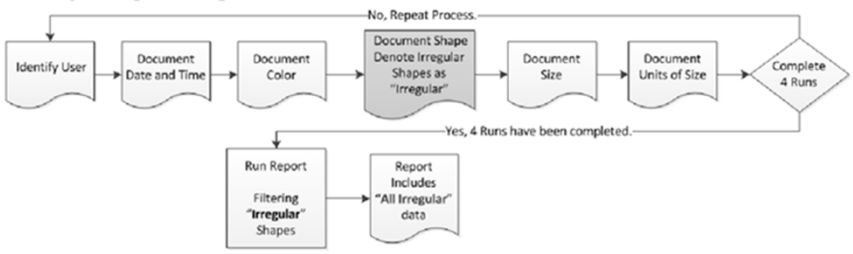
Complete data includes **data from all the actions taken** to obtain the required information.

Complete - Expectations

- Complete data includes **all data and all its metadata** generated to capture its creation and its modifications.
- Complete data **should be**:
  - **A**ttributable – shows who create what data
  - **L**egible – data is readable
  - **C**ontemporaneous – shows when data was created
  - **O**riginal – maintains the original reads
  - **A**ccurate – shows all the correct data

Data Integrity - Consistent

Are you getting consistent data?



Data Run	User	Date	Time	Color	Shape	Size	Units
1	T. Thumb	12-Aug-2014	8:12:00 AM	Green	Square	10.2	cm
2	J. Little	12-Aug-2014	8:25:00 AM	Purple	**Irregular**	9.8	cm
3	T. Thumb	12-Aug-2014	9:12:00 AM	Green	Irregular	7.8	cm
4	J. Little	12-Aug-2014	10:03:00 AM	Green	Square	9.9	cm

Consistent data should be created in a manner that **can be repeated**.

Consistent - Expectations

- Consistent data is data that is **created in a repeatable method**.
  - **Well documented process** controls must be established. (i.e. , procedural controls, methods, bath records, etc.)
  - **Good Documentation Practices** must be implemented, utilized, and periodically reviewed.
  - Personnel creating data must be **appropriately trained** to perform the tasks **per the described tasks**.
- Consistent data is
  - **L**egible – data is readable
  - **C**ontemporaneous – shows when data was created
  - **A**ccurate – shows all the correct data

Data Integrity - Enduring

Do you well store all your Data?

Enduring data must be protected from loss, damage and/or alteration and must be available throughout the defined retention period.

Enduring - Expectations

- Data should be stored on a medium that endures **the entire retention period**
- Data backups and original data should be **stored in different locations.**
- **Periodic review of media integrity** should be performed to ensure data can be recovered and read throughout retention period.
- Enduring data is:
  - **L**egible – data is readable
  - **O**riginal – maintains the original reads

Data Integrity - Available

Could you retrieve all your valid Data?

Available data is readily retrieved throughout the lifecycle of the system, or the appropriate retention period

Available - Expectations

- Data must be available and **in human readable form**.
- **Timely availability** of data is important, especially when requested during an audit.
- Improvement to systems, may impact current data, ensure data is still accessible, usable and readable **during and after the upgrade**.
- Complete data **should be**:
  - **A**ttributable – shows who create what data
  - **L**egible – data is readable
  - **C**ontemporaneous – shows when data was created
  - **O**riginal – maintains the original reads
  - **A**ccurate – shows all the correct data

ALCOA & ALCOA + Characterize Data Integrity

In order to have Data Integrity, data must be:

- **A**ttributable
- **L**egible
- **C**ontemporaneous
- **O**riginal
- **A**ccurate
- Complete
- Consistent
- Enduring
- Available

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

For Example

- IT policies.
- System administration (access right, roles and privileges).
- Data management.
- Data acquisition and processing.
- Data review and approval.
- Date archiving.
- Anti-fraud monitoring.

IT policies

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

IT policies - Expectations

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.

System administration

- The auditor will want to understand how access to the instrument is authorised and controlled.
- You need to justify the access levels within the instrument and the user privileges at each level.
- 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.

System administration - Expectations

- Audit Trail functionality is switched ON within the Instrument Admin console.

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

System administration – Expectations

- Specific privileges within the user profile
  - data cannot be deleted by a user once acquired.
  - data can be moved to a different folder to potentially “hide” it. (e.g. trial injections)
  - electronic data that has been processed must be saved before it can be submitted for review/printed out.

- Administration reports:
  - Active users
  - User privileges
  - Administration audit trail report

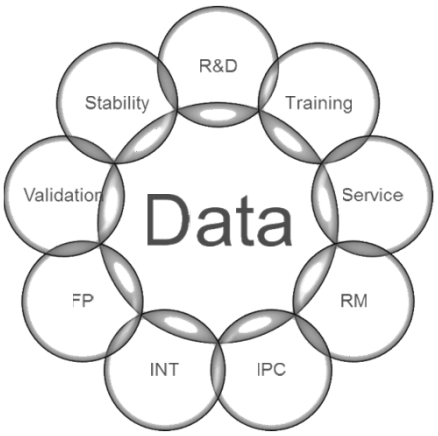
Data Management

The auditor will want to understand

- How data is managed within the instrument and check that users are following the internal procedure.
- The data management structure that segregates different types of data and enables easy retrieval during the audit.

Data Management - Expectations

- Segregate GMP release data is from Research / Development data if you have dual functionality within your organisation using the same Instrument.
- Data structure - Consider what types of data you produce and decide how each type of data should be stored within the instrument.



Data Acquisition and Processing

Data Processing Risks:

- Main area where results can be manipulated by human intervention.
- Target area for auditors.
- Multiple reprocessing.

Data Acquisition and Processing - Expectation

- All data processing should be performed within the instrument 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.
- Use pre-defined integration parameters wherever possible to avoid manual integration of multiple peaks.

Data Acquisition and Processing - Expectation

- Chromatography should be presented on an appropriate scale so that integration is clearly visible.
- Disable annotation tools within the instrument which could be used to deliberately alter the appearance of the chromatograms.
- Save all changes to individual chromatograms, sequences and processing methods before submitting for review.
- Ensure that accurate audit trail comments are entered into the instrument when prompted to provide traceability.

Data review and approval - Expectation

- Test 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 and approval - Expectation

- 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.

Data review and approval – 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.

Data review and approval – Auditor Checklist

- Lab Demo – User log-on (multiple), date / time locked, cant delete data.
- 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.

Data review and approval – Auditor Checklist

- Training – assess staff competency with instrument in lab. Make sure staff are trained to interact with the auditor. Have a instrument super- user present during the lab inspection.
- Query search –assurance that batch hasn't been analysed multiple times as part of an investigation.
- Final electronic results in instrument match those reported on CofA.

Date archiving

- Periodic GMP data archiving – make sure that data archiving is defined in your procedure and performed regularly.
- Minimizes 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.

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 instrument to perform audit trail review before GMP
- batch release.

Can you answer the 5 key Data Integrity questions now?

- 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?

Professional Attitude

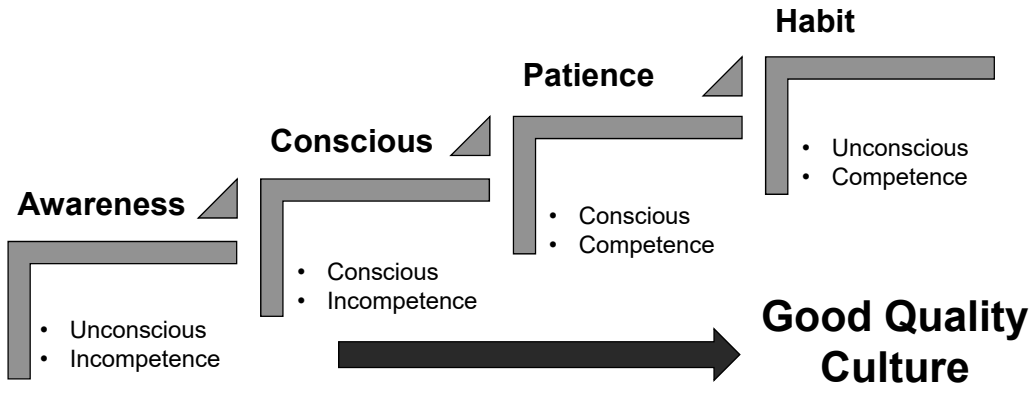
Unprofessional

- Feel embarrassed after making a mistake
- Admission of error – harmful
- Covering up- Why admit when nobody is watching

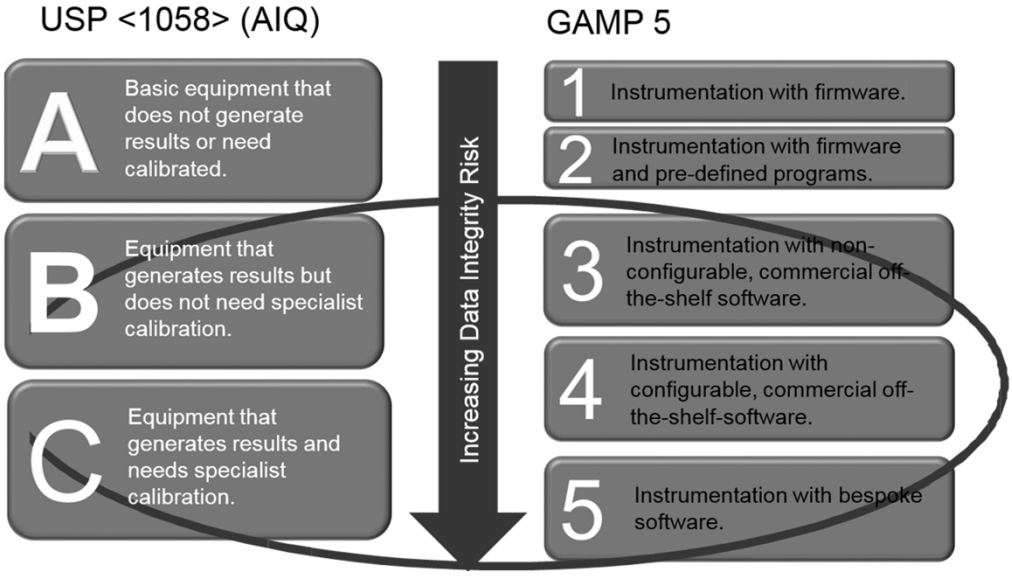
Professional

- Put errors to good use
- Share with others
- Analyse and find Root Cause
- Correct errors through QMS
- Anticipate that errors will be made in the learning process
- Risk acceptance: It needs to be understood that errors may occur

Professional Attitude - Expectation



Data Integrity – Risk Assessment



High Risk Instrument Type

Category	Classification	Qualification Approach	Some Examples
A Low Risk	**Standard equipment,** no measurement capability or requirements for calibration	Conformance with requirements verified and documented by observation of operation.	▪ Magnetic stirrers ▪ Vortex mixers ▪ Sonic baths ▪ Shakers ▪ Class A Pipettes ▪ Nitrogen Evaporators
B Medium Risk	**Standard instruments** with measurement values or control physical parameters	User requirements typically within unit functions. Require calibration. Conformance to requirements via SOPs, Calibration Verification / Certificates, and IQ/OQ.	▪ Balances ▪ pH Meters ▪ Thermometers ▪ Timers ▪ Pumps ▪ Water baths ▪ Centrifuges ▪ Light Microscopes ▪ Variable Pipettes
C High Risk	**Complex instruments** and computerized systems	Full qualification process required. Specific function and performance tests	▪ HPLC, LCMS, GC, GCMS ▪ ICP-MS, AA, Analyzers ▪ Dissolution, UV/Vis ▪ Particle Analyzers, Densitom. ▪ Robotic Systems ▪ FTIR, DSC, TGA, SEM, TEM ▪ Autoclaves, Stability Chamb. ▪ Refrig, Freezers, Incubators

Medium Risk Instrument Type

Category	Classification	Qualification Approach	Some Examples
A Low Risk	**Standard equipment,** no measurement capability or requirements for calibration	Conformance with requirements verified and documented by observation of operation.	▪ Magnetic stirrers ▪ Vortex mixers ▪ Sonic baths ▪ Shakers ▪ Class A Pipettes ▪ Nitrogen Evaporators
B Medium Risk	**Standard instruments** with measurement values or control physical parameters	User requirements typically within unit functions. Require calibration. Conformance to requirements via SOPs, Calibration Verification / Certificates, and IQ/OQ.	▪ Balances ▪ pH Meters ▪ Thermometers ▪ Timers ▪ Pumps ▪ Water baths ▪ Centrifuges ▪ Light Microscopes ▪ Variable Pipettes
C High Risk	**Complex instruments** and computerized systems	Full qualification process required. Specific function and performance tests	▪ HPLC, LCMS, GC, GCMS ▪ ICP-MS, AA, Analyzers ▪ Dissolution, UV/Vis ▪ Particle Analyzers, Densitom. ▪ Robotic Systems ▪ FTIR, DSC, TGA, SEM, TEM ▪ Autoclaves, Stability Chamb. ▪ Refrig, Freezers, Incubators

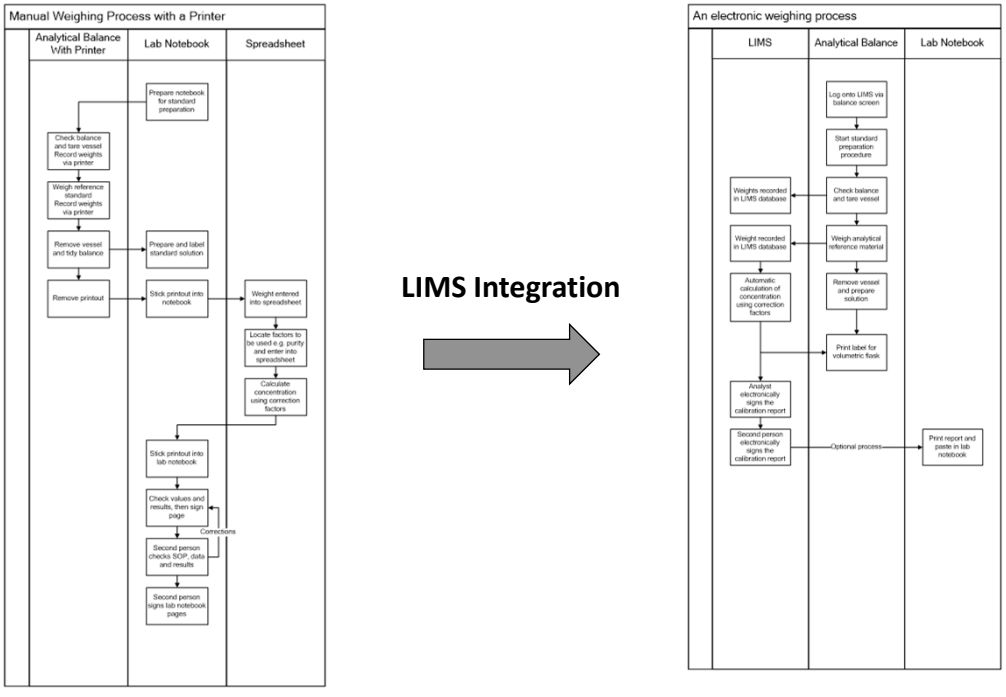
To increase integrity in the laboratory

- Implement **Risk based** processes
- Define a **single** point of truth for meta data
- **Reduce**, **automate** & **simplify** workflow complexities
- Stop **spreadsheet madness**
- Implement **self-documenting** process at the source
- Utilize **best practice** analysis protocols
- Adopt and use data **industry** standard & process
- **Avoid** custom software extension

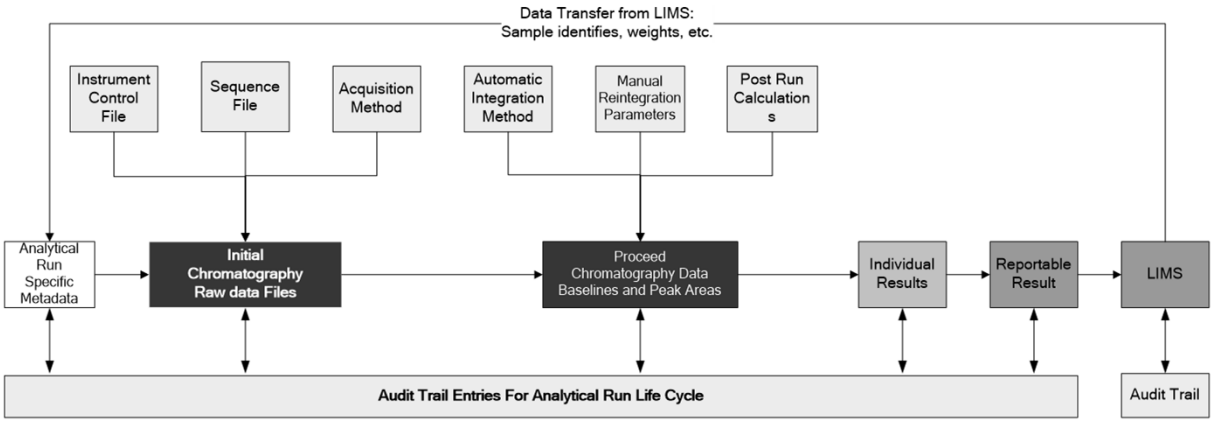
How Can LIMS Help Ensure Data Integrity

LIMS Features that address data integrity issues

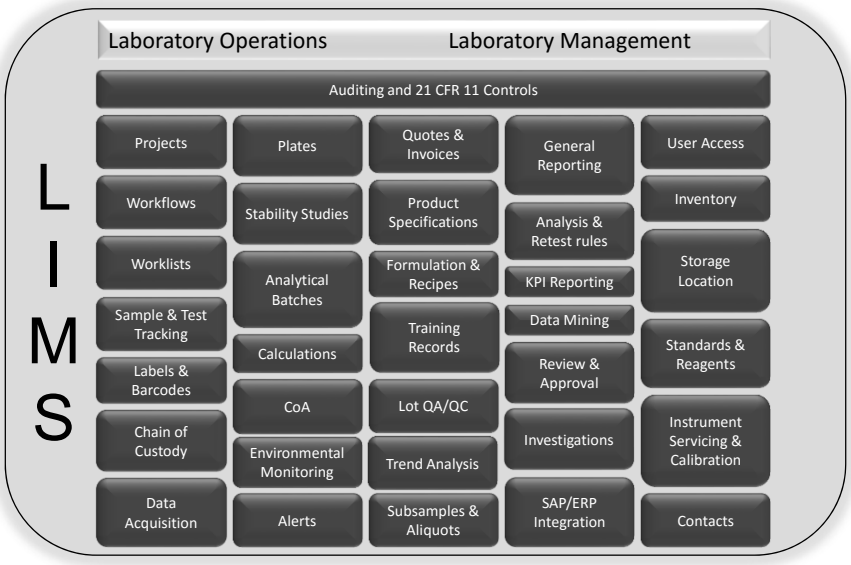
- User access control
- Group/Role security
- ERES
- Audit Trails
- Secure Reporting
- Unique identifiers
- Version control
- Chain of Custody
- ISO 17025



LIMS and CDS interfaced to work electronically



Full Featured LIMS



Data Management Software

Commonly used in laboratories:

- (CDS) Chromatography Data Systems (CDS)
- (DAS) Other Data Acquisition Systems (DAS)
- (LIMS) Laboratory Information Management Systems (LIMS)
- (ELN) Electronic Laboratory Notebooks (ELN)
- (DMS) Document Management Systems (DMS)
- (CAPA) Corrective Action Preventive Action (CAPA)
- Trail
- 21 CFR 11
  - Electronic Records
  - Electronic Signatures

115

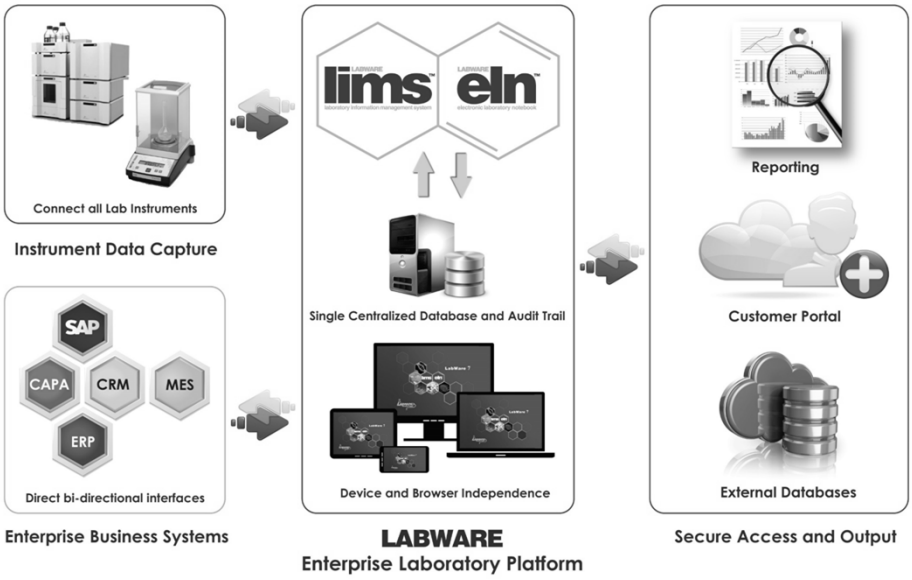
Data Management Software

Understand how these systems are used

- What are their limitations?
- How are they integrated?
- User access controls
- Audit Trails
- Chain of Custody

116

LabWare ELP



LIMS EXPERIENCE

Maintaining Compliance

Maintaining Compliance

What are some specific trigger events that should cause a organization to re-evaluate laboratory data integrity and regulatory compliance?

- When a regulatory agency publishes a new data integrity guidance document
- If your organization makes a major policy or process change related to record retention
- A new business partner or supplier creating, storing, or otherwise processing regulated data on your behalf
- A Merger or acquisition has occurred

Q & A