GMP FORUM 2023

Data integrity & related laboratory deficiencies

Gaye Camm

Senior GMP Inspector – Technical Specialist

Manufacturing Quality Branch

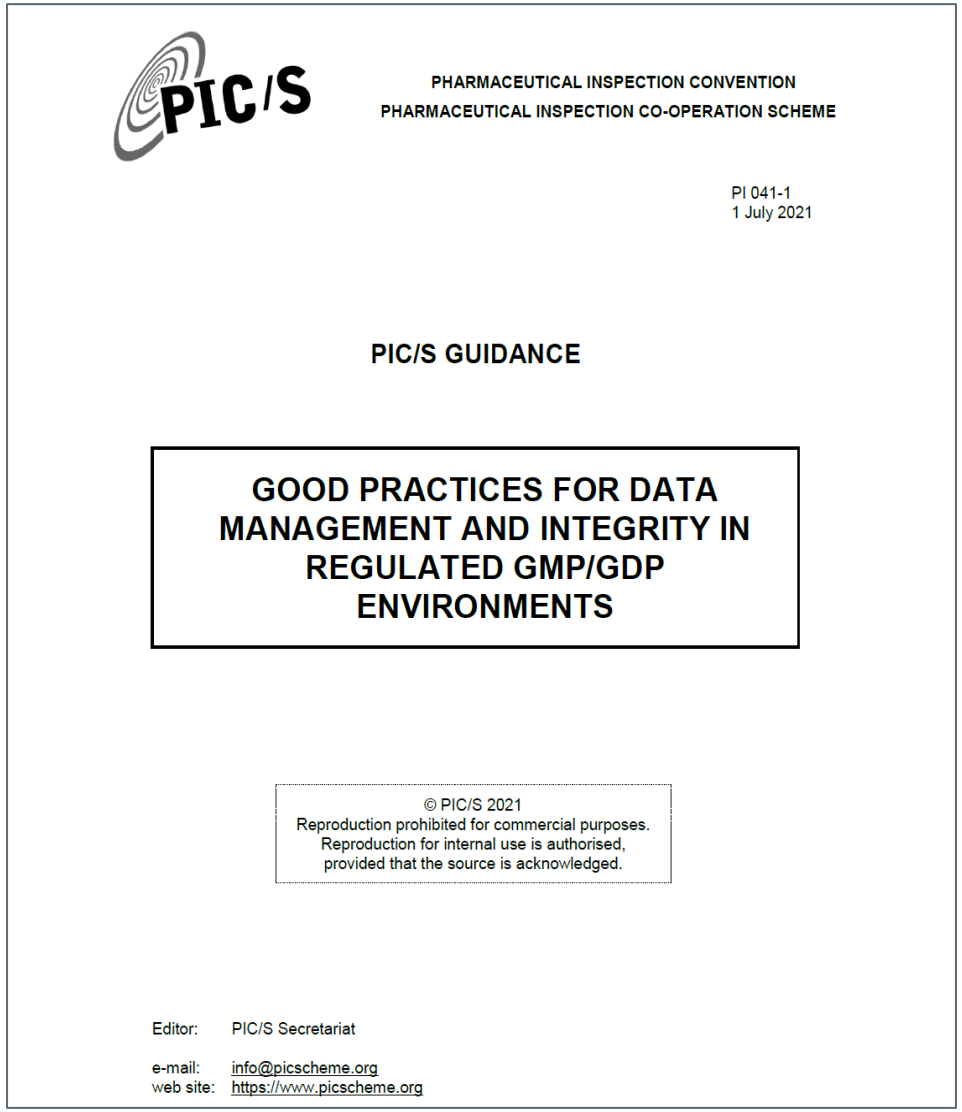
Department of Health and Aged Care, TGA

What is Data Integrity?

The degree to which data are:

- Complete
- Consistent
- Accurate
- Trustworthy
- Reliable

…and these characteristics of the data are maintained through the data life cycle.



PIC/S

PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 041-1
1 July 2021

PIC/S GUIDANCE

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

Editor: PIC/S Secretariat

e-mail: info@picscheme.org
web site: https://www.picscheme.org

ALCOA+ Principles

A – Attributable

- Clearly identify who performed a recorded task and when the task was performed
- Applies to changes, corrections & deletions

L – Legible

- It must be possible to read or interpret the data after it is recorded
- Permanent
- Software available to interpret data if in dynamic format

C – Contemporaneous

- Data, or evidence of actions, events or decisions should be recorded as they take place

O – Original

- The original record is the first-capture of information
- Data must be preserved in its unaltered state

A – Accurate

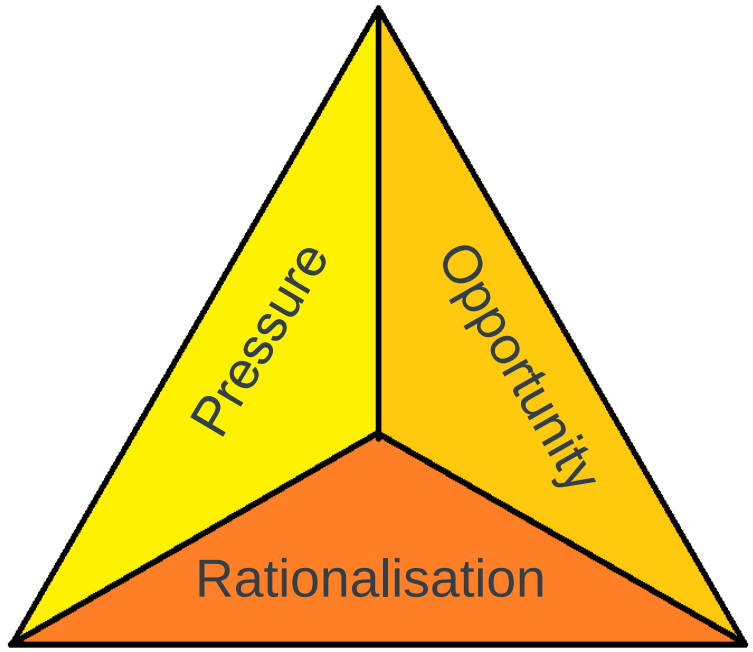
- Data must truthfully represent the action / observation made
- Data checked where necessary
- Supported by robust PQS

+ – Plus

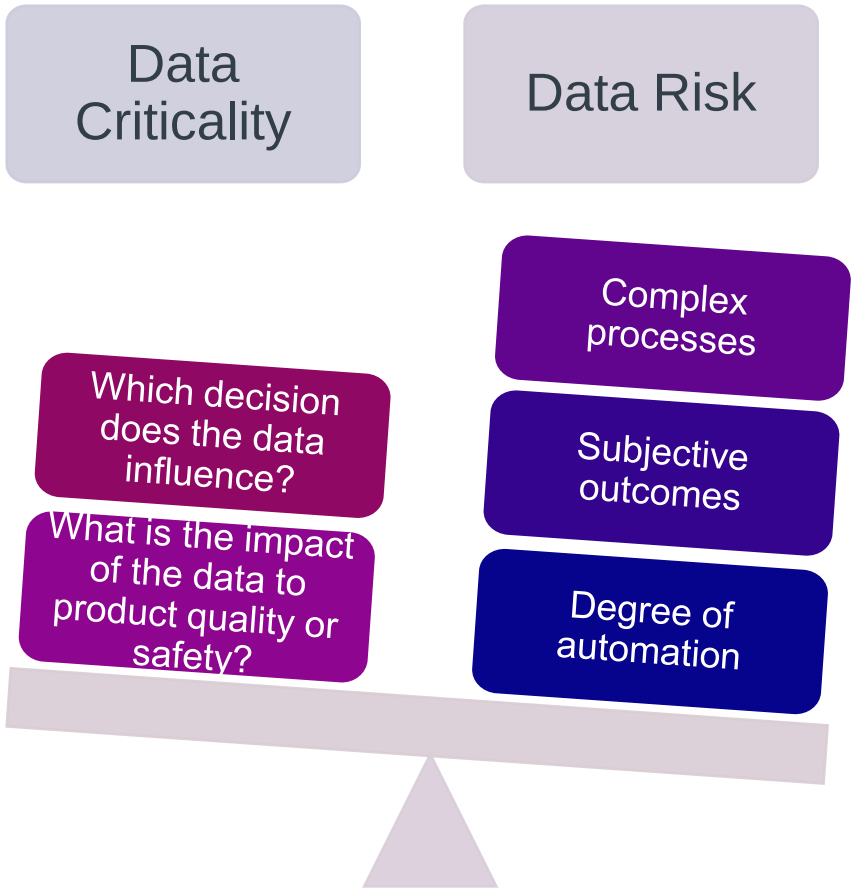
- Complete
- Consistent
- Enduring
- Available

Creating the right environment

- Data management controls embedded in PQS
  - System design to ensure good DI practices
  - QRM approach to data integrity
  - Ongoing risk review of data criticality vs. risk
  - Robust self inspection program
- Clear understanding of importance of data integrity at all
  levels of the organisation
- Internal reporting encouraged & supported by Management
- Mature, open management approach to data integrity



Risk management approach to Data Integrity



Data Criticality

- Batch release data > cleaning records
- Data relating to product quality/safety

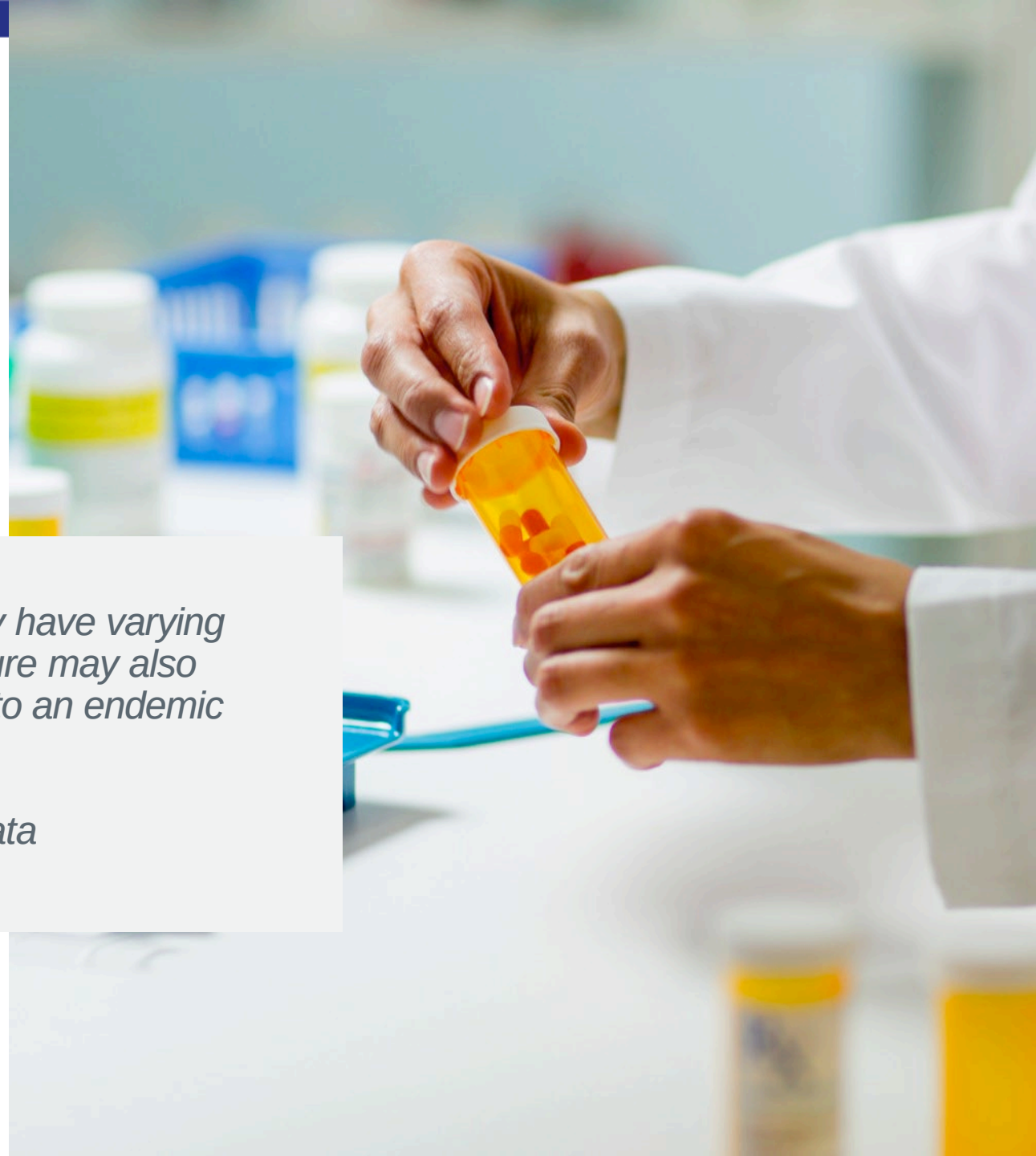
Data Risk

- Vulnerability of data to alteration, deletion, recreation, loss or deliberate falsification

Desired outcome = effective control strategy to manage identified risks

Where does it go wrong?

Data integrity issues seen during TGA inspections



- *Deficiencies relating to data integrity failure may have varying impact to product quality. Prevalence of the failure may also vary between the actions of a single employee to an endemic failure throughout the inspected organisation.*
- *- PIC/S guidance - PIC/S Good Practices for Data Management and Integrity PI 041*

Data integrity in microbiological laboratories

Manipulation of data

- No testing conducted
- Not counting all colonies
- OOS data not being investigated
- Resampling/retesting without justification

Incomplete Testing

- Samples not taken or “lost” in transit
- No reconciliation of samples
- Incubation conditions incorrect
- Using unvalidated test methods

Poor test records

- Not recording all key test data
- Worksheets ripped up and replaced
- No reconciliation of forms used
- Lack of proper computerised system security
- Colony morphology not matching identification results

Competence/supervision | Effective controls | Secondary Checks | Computerised system configuration | Organisational Culture / resources

Data integrity controls for manual test methods

Sampling Procedures

- Sampling schedule/plans
- Training of technicians
- Sample forms
- Detailed collection methods
- Identity of sampler recorded

Test methods

- Test volumes/weights recorded
- Calibrated equipment used
- Reference to all reagents
- Reference to validated methods/dilution factors
- Samples processed under clean conditions, e.g. LAF
- Negative controls for processed samples
- Identity of tester/equipment recorded

Incubation

- Incubation records maintained
- Min/max incubation time defined and validated
- All transfers/sub-culturing recorded
- All incubated samples tagged and identified

Reading results

- Technicians trained in detection, enumeration and morphology – clear SOPs, photos
- Controlled environment for reading, light, magnification
- Counting device used for colonies
- Clear acceptance criteria/limits
- OOS & ID policy for manual recording
- All samples reconciled
- Results recorded
- Calculations applied correctly
- Second checks and verification in accordance with quality risk management

Computerised Systems

*Annex 11 §4.3 An up-to-date listing of all **relevant systems** and their **GMP functionality** (inventory) should be available. For critical systems, an up-to-date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.*

- No consolidated listing available
- Missing information e.g. PLC controlled equipment, simple testing instruments such as auto titrators
- Interfaces with other systems or processes not documented

Questions to consider when determining GMP criticality

- Does the system control the purchasing and/or status of products and materials?
- Is it used for control and/or data acquisition for critical manufacturing processes or testing activities?
- Does the system generate, store or process data that are used to determine batch quality?
- Will the system generate data that are included in the batch processing or packaging records?
- Is the system used in the decision process for the release of products?
- Do you have simple systems that generate initial records in electronic format?

Excel spreadsheets and ALCOA requirements

- Permit multiple users without providing ability to attribute entries to a specific person (Attributable)
- Data can be accidently or maliciously over-written and/or replaced (Legible)
- Does not record when data entries have been made (Contemporaneous)
- Multiple copies can be made of an Excel spreadsheet outside of the documentation system (Original)
- Formulae and other functions have potential to be corrupted without being detected (Accurate)

Laboratory Electronic systems

Validation

- Software validation
- Hardware qualification
- Configuration management
- Change management
- Periodic system review

Configuration

- Audit Trails
- OS security
- Data back-up/archiving
- Test method configuration

User Access

- SOPs for user access control
- Individual user access
- Defined user privileges
- System administrator

Data management

- Data review SOPs
- Raw data verification
- External calculation tools
- Audit trail review
- E-signatures

Computerised system should be verified for intended use

- No URS available for newly installed computerised systems
- Documentation supplied with commercial off-the-shelf products not reviewed to ensure user requirements are fulfilled
- Validation reports for critical system contained inadequate system descriptions:
  - data flows and interfaces with other systems or processes
  - hardware and software pre-requisites
  - security measures required for DI

Control of standalone systems

- Back up of electronic data poorly administered
- Time & date on computer can be modified by user
- Unique user logins not implemented for all staff
- Inappropriate use of ‘Administrator’ login
- Data can be deleted directly from hard drives without detection

Annex 11 §9: Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented.
Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

- Audit trail not regularly reviewed
- Audit trail review conducted on select data only
- Review requirements not formalised in procedures
- Orphan data not captured in analysis
- Reconciliation of electronic data with associated logbooks not considered

Audit trail review

- Considerations
  1. Periodic review of system wide changes e.g. users, system settings
  2. Routinely review for potentially damaging user behaviours
     - Unauthorised changes to test methods or instrument settings
     - Undocumented manual manipulation of data e.g. integration, calibration, calculated values
     - Explanation for ALL data on the system, including data that is not reported
- Procedure for audit trail review, including frequency
- Process for recording the results of audit trail review
- Deviations from standard procedures or atypical results should be investigated

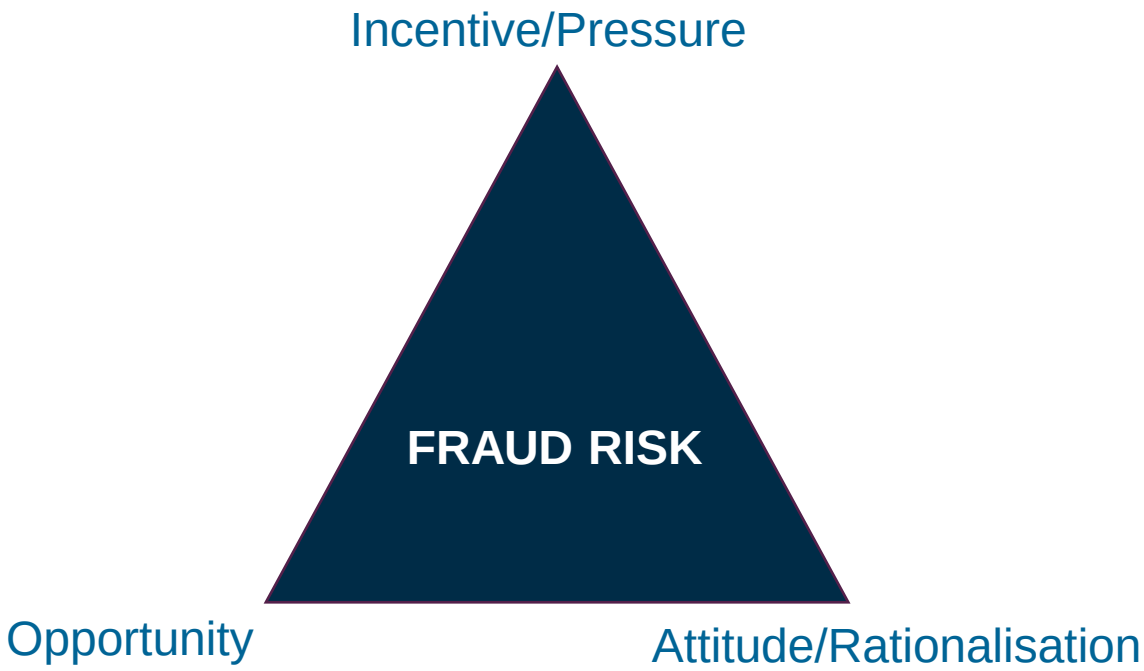
Third party suppliers of cloud services (IaaS, PaaS, SaaS)

- No risk assessment conducted to identify risk associated with using third parties who are creating, processing or storing regulated data
- No supplier assessment of cloud service providers conducted
- No formal agreement in place between the manufacturer and cloud service provider outlining GMP responsibilities

Search for ‘SOC 2 Assessment of GxP Suppliers of IT Services’

Regulatory expectations

- Design systems to prevent data integrity issues
- Ensure the data is authentic and retrievable
- Train staff and encourage correct behaviours and practices
- Open communication
- Encourage feedback
- Build a system for ongoing review



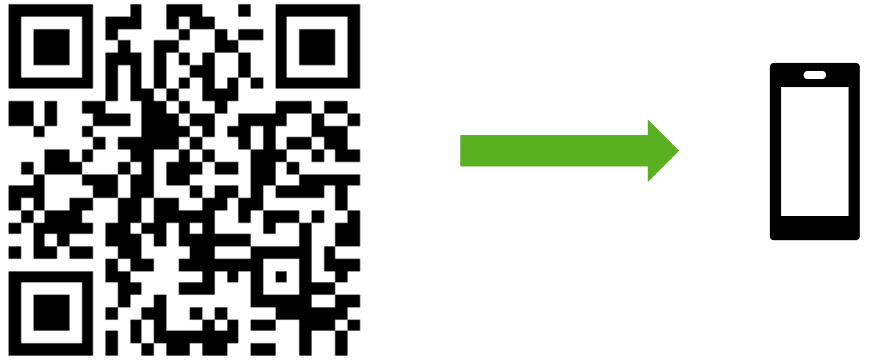
How to ask questions

Verbal questions:

Raise your hand to ask a verbal question. A member of the GMP Forum staff will provide a roaming microphone.

Written questions:

Scan the QR code below or click the link in your calendar to access Slido via your mobile device. You can submit your question, and vote on other questions submitted.



Australian Government

Department of Health and Aged Care

Therapeutic Goods Administration

Coming up next in this room

Paul Stephney

Senior Inspector and Technical Specialist

GMP for listed Medicines