

Data Integrity



Data Integrity

Increased Regulatory Oversight

MHRA

FDA

Health
Canada

WHO

PIC/S

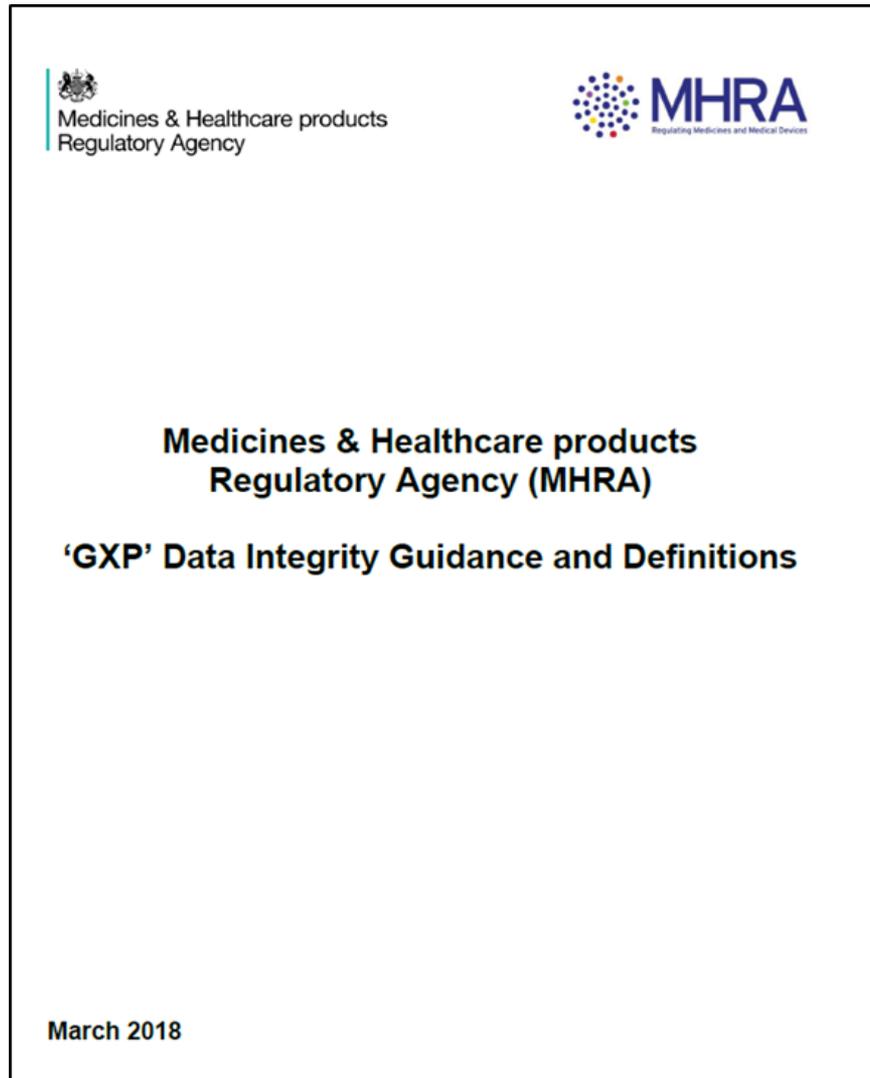
GAMP



Data Integrity

May 2018

3



https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf



The way regulatory data is generated has continued to evolve in line with the ongoing development of supporting technologies such as the increasing use of electronic data capture, automation of systems and use of remote technologies; and the increased complexity of supply chains and ways of working, for example, via third party service providers.

Systems to support these ways of working can range from manual processes with paper records to the use of fully computerised systems. The main purpose of the regulatory requirements remains the same, i.e. **having confidence in the quality and the integrity of the data generated** (to ensure patient safety and quality of products) and **being able to reconstruct activities**.



Data Integrity

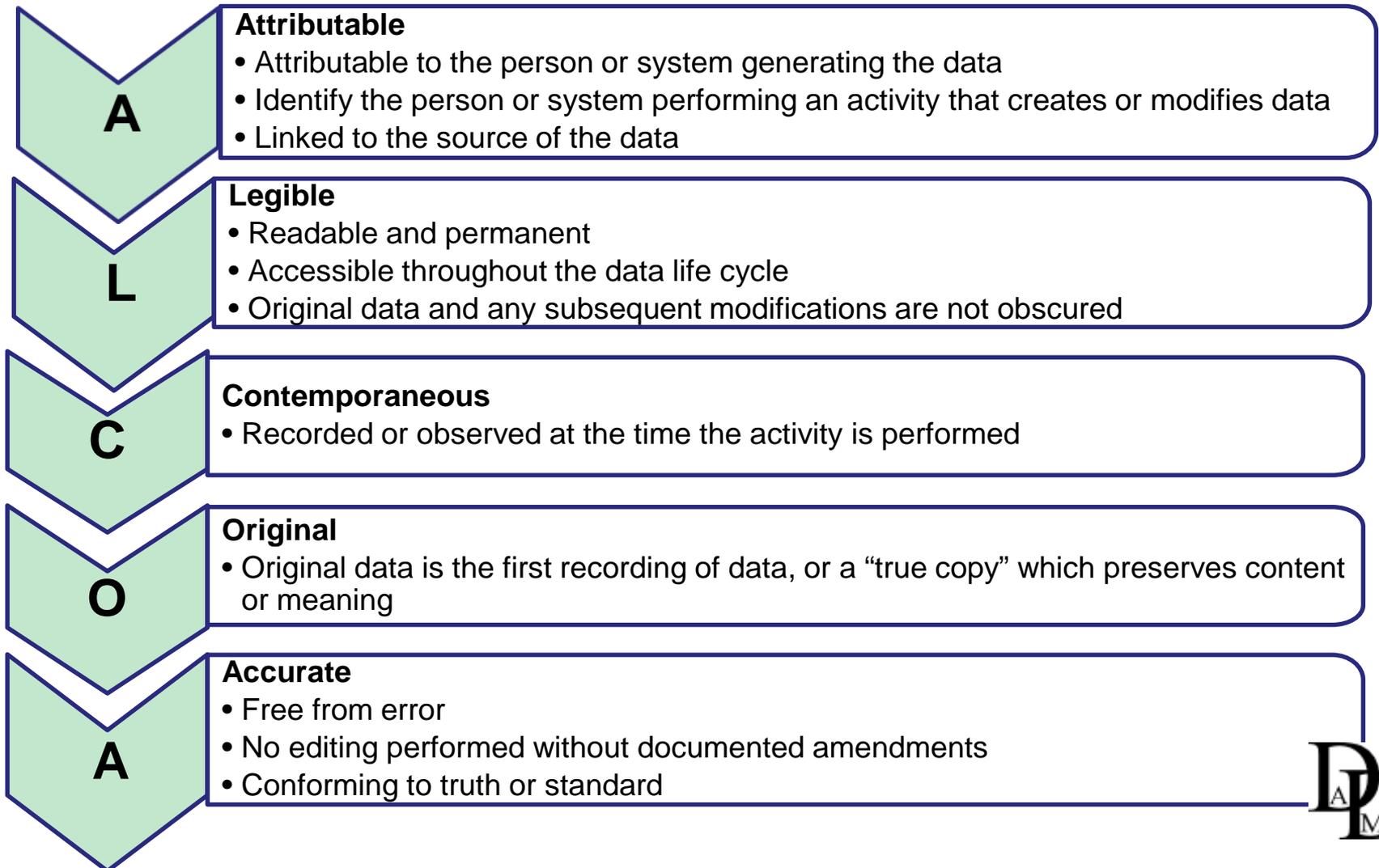
- The extent to which all data are complete, consistent, accurate, trustworthy and reliable throughout the data lifecycle

Data Governance

- The mechanisms to ensure data integrity:
 - Processes and systems
 - Training
 - Working environment/culture
 - Monitoring etc

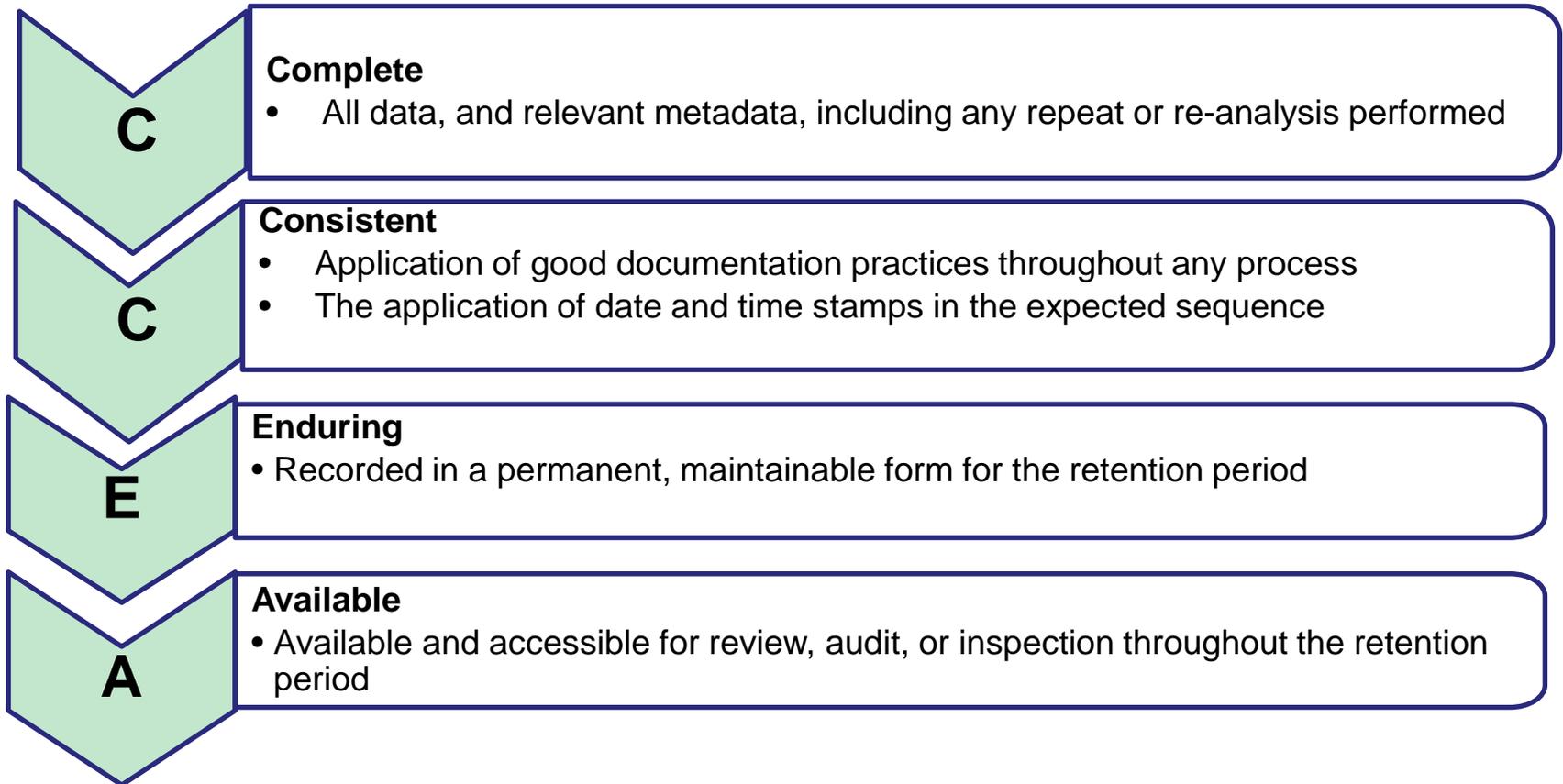
Data Integrity

- Data should be:



Data Integrity

- Data governance should ensure:



Data Integrity

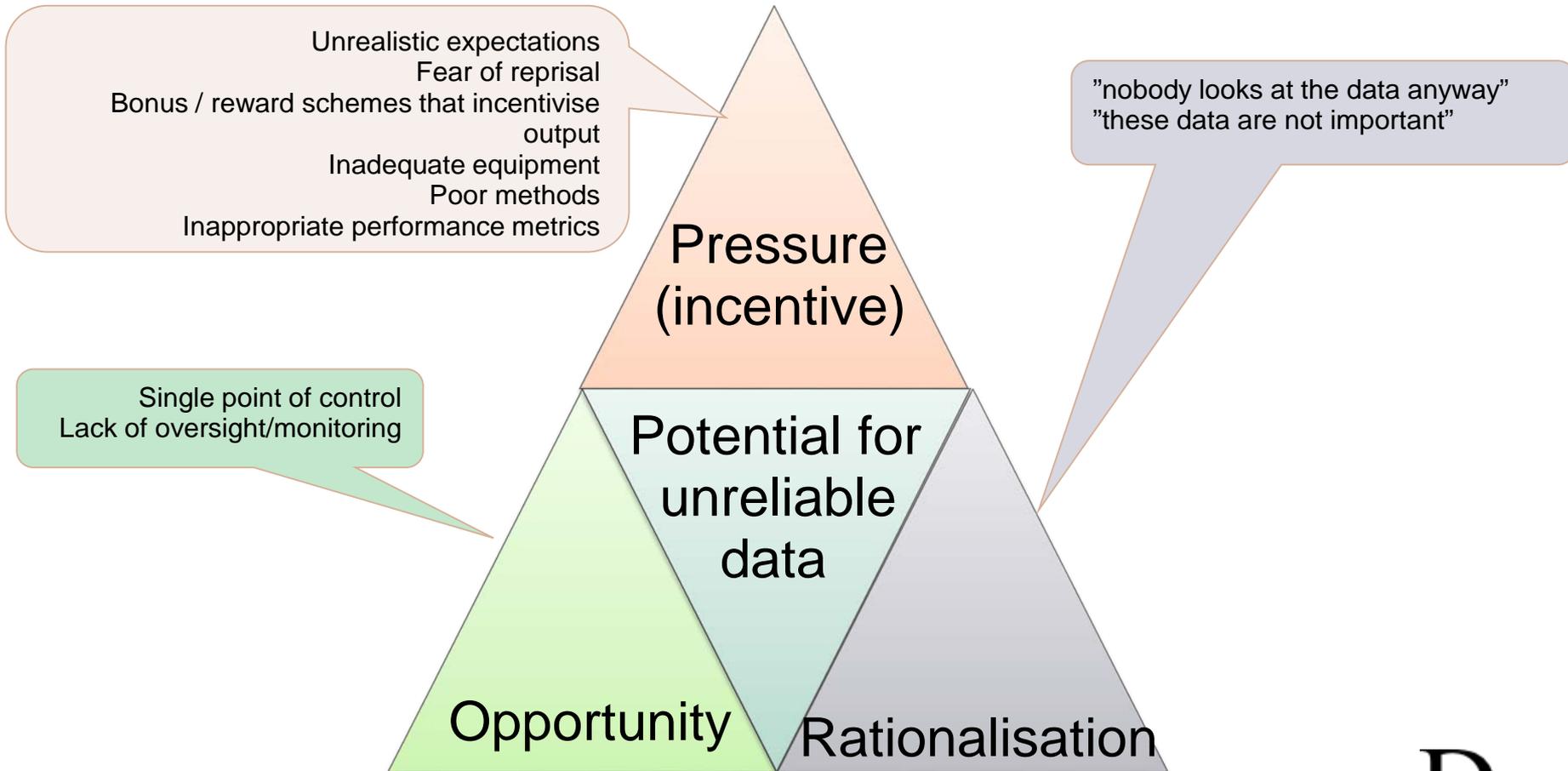
- Risks to data integrity

Range from non-intentional to intentional incidents e.g:

- Slips and lapses that are just part of being human
- Mistakes that are made because there are insufficient controls or too much complexity
- Situational violations that occur when something unexpected happens and we just do the wrong thing
- Routine violations that involve doing the wrong thing over and over because it is easier and we think that taking that shortcut does not matter
- Optimized violations that are concerned ways of working to avoid a control and/or evade associated additional workload
- Intentionally misleading activities that are actions to cover unauthorized manipulation of data and fraud



Data Integrity – the Cressey Triangle



- Design systems and processes to prevent Data Integrity issues
- Employ a risk-based approach that includes data risk, criticality and lifecycle to identify data with greatest GXP impact
- Train staff to encourage correct behaviours/practices
- Encourage feedback (don't shoot the messenger)
- Ensure ongoing review/monitoring



Data Integrity

Points to consider

Where the capability of the electronic system permits dynamic storage, it is not appropriate for static (printed / manual) data to be collected in preference to dynamic (electronic) data.

Data must be retained in a dynamic form where this is critical to its integrity or later verification.

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.



Data Integrity

DATA RISK ASSESSMENT

Perform a 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.

The DIRA (or equivalent) should consider not only the computerised system but also the supporting people, guidance, training, and quality systems.

Where there is human intervention, particularly influencing how or what data is recorded, reported or retained, an increased risk may exist from poor organisational controls or poor data verification.



Data Integrity

DATA REVIEW

- There should be a procedure that describes the process for the review and approval of data. Data review should also include a risk-based review of relevant metadata, including relevant audit trail records.
- Data review should be documented and should include a positive statement regarding whether issues were found or not, the date that review was performed and the **signature of the reviewer**.
- The relevance of data retained in audit trails should be considered by the organisation to permit robust data review/verification. It is not necessary for audit trail review to include every system activity (e.g. user log on/off, keystrokes etc.).
- Routine data review should include a documented audit trail review where this is determined by a risk assessment. When designing a system for review of audit trails, this may be limited to those with GXP relevance.
- Reviewers should have sufficient knowledge and system access to review relevant audit trails, raw data and metadata.



DATA REVIEW

- In-process audit trail reviews should be documented in the same way in which data reviews are documented, and should be described just as in the use procedures corresponding to the system.
- On a maintenance process level, in-process audit trail reviews should also be integrated into the periodic user account review process, for example, to scan for any occasions where a normal user was given administrator rights for a short period of time.
- Another type of in-process audit trail review should be performed as part of routine system maintenance by IT administrators. These should include checks as to whether or not the audit trail is still functional and has never been disabled, and if the system clocks used are working correctly. This can also cover a review of back end changes, which are typically not logged in application layer audit trails but may be recorded at the database level.
- As with any risk-based activities, it can also be determined for a specific system that no in-process audit trail reviews are needed. In such cases, a risk assessment should document the justification for that conclusion.



Data Integrity

COMPUTERISED SYSTEM ACCESS

Companies must be able to demonstrate the access levels granted to individual staff members and ensure that historical information regarding user access level is available.

System administrator access should be restricted to the minimum number of people possible. The generic system administrator account should not be available for use. Personnel with system administrator access should log in with unique credentials that allow actions in the audit trail(s) to be attributed to a specific individual.

System Administrator rights (permitting activities such as data deletion, database amendment or system configuration changes) should not be assigned to individuals with a direct interest in the data (data generation, data review or approval).



Data Integrity

VALIDATION // CLOUD PROVIDERS

The acceptance of vendor-supplied validation data in isolation of system configuration and users intended use is not acceptable.

The physical location where the data is held, including impact of any laws applicable to that geographic location should be considered.

Appropriate arrangements must exist for the restoration of the software/system as per its original interactive validated state, including validation and change control information to permit this restoration.



Senior management should be accountable for the implementation of systems and procedures to minimise the potential **risk** to data integrity, and for identifying the **residual risk**.

Contract Givers should ensure that data ownership, governance and accessibility are included in a **contract/technical agreement**. The Contract Giver should also perform a data governance review as part of their vendor assurance programme.



Data Integrity

