



1  
2 **MHRA GxP Data Integrity Definitions and Guidance for Industry**

3  
4 **Draft version for consultation July 2016**

5  
6  
7  
8  
9 **Background**

10  
11 The way in which regulatory data is generated has continued to evolve in line with the introduction  
12 and ongoing development of supporting technologies, supply chains and ways of working. Systems  
13 to support these ways of working can range from manual processes with paper records to the use of  
14 computerised systems. However the main purpose of the regulatory requirements remains the same;  
15 having confidence in the quality and the integrity of the data generated and being able to reconstruct  
16 activities remains a fundamental requirement.

17  
18  
19 **Introduction:**

20  
21 This document provides guidance on the data integrity expectations that should be considered by  
22 organisations involved in all aspects of the chemical<sup>1</sup> and pharmaceutical development lifecycle.

23  
24 This guidance should be read in conjunction with the applicable regulations and the general guidance  
25 specific to each GxP. Where GxP-specific references are made within this document (e.g. ICH Q9),  
26 consideration of the principles of these documents may provide guidance and further information.

27  
28 Arrangements in place within an organisation with respect to people, systems and facilities should be  
29 designed, operated and where appropriate adapted to support a working environment and  
30 organisational culture that ensures data is complete consistent and accurate in all its forms, i.e. paper  
31 and electronic. The effort and resource applied to assure the validity and integrity of the data should  
32 be commensurate with the risk and impact of a data integrity failure to the patient or environment.  
33 When taken collectively these arrangements fulfil the concept of data governance.

34  
35 Organisations are not expected to implement a forensic approach to data checking on a routine basis,  
36 but instead design and operate a fully documented system that provides an acceptable state of  
37 control based on the data integrity risk with supporting rationale. In addition to routine data review, the  
38 wider data governance system should ensure that periodic audits are capable of detecting  
39 opportunities for data integrity failures within the company's system, e.g. routine data review should  
40 consider the integrity of an individual data set, whereas the periodic system review might verify the  
41 effectiveness of existing control measures and consider the possibility of unauthorised activity.

42  
43 It should be noted that data integrity requirements apply equally to manual (paper) and electronic  
44 data. Organisations should be aware that reverting from automated / computerised to manual / paper-  
45 based systems will not in itself remove the need for appropriate data integrity controls. Where data  
46 integrity weaknesses are identified, either as a result of audit or regulatory inspection, companies with  
47 multiple sites should ensure that appropriate corrective and preventive actions are implemented

---

<sup>1</sup> Chemical lifecycle relating to GLP studies regulated by MHRA



48 across the organisation. Appropriate notification to regulatory authorities should be made where  
49 applicable.

50  
51 Although not included in this guidance, the impact of organisational culture and senior management  
52 behaviour on the success of data governance measures should not be underestimated.

53  
54 **Establishing data criticality and inherent integrity risk:**

55  
56 The degree of effort and resource applied to the organisational and technical control of data lifecycle  
57 elements should be commensurate with its criticality in terms of impact to quality attributes.

58  
59 Data may be generated by (i) manual means - a paper-based record of a manual observation, or (ii)  
60 electronic means - in terms of equipment, a spectrum of simple machines through to complex highly  
61 configurable computerised systems.

62  
63 When manually recorded data requires stringent oversight, consideration should be given to risk-  
64 reducing supervisory measures. Examples include contemporaneous second person verification of  
65 data entry, or cross checks of related information sources (e.g. equipment log books).

66  
67 The inherent risks to data integrity relating to equipment and computerised systems may differ  
68 depending upon the degree to which data (or the system generating or using the data) can be  
69 configured, and therefore potentially manipulated (see figure 1).

70  
71  
72  
73  
74  
75  
76  
77

DRAFT



78  
79  
80  
81

**Figure 1: Table to illustrate the spectrum of simple machine (left) to complex computerised system (right), and relevance of printouts as ‘original data’**

System complexity	Simple system					Complex system
	pH meter	Filter integrity test			Interactive response technology	Enterprise resource planner
		UV spec	HPLC systems	LC-MS-MS	LIMS	
	Balance	FTIR		Pharmacovigilance database		Bespoke systems
		ECG machines	Electronic trial master file		Clinical database	
		Spreadsheet			Statistical analysis tools	
	Min/Max thermometers	Data loggers	Building management system			
<b>Software</b>	No software	Simple software				Complex software
<b>Printouts</b>	Printouts may represent original data	Printouts not representative of original data				

82  
83

With reference to figure 1, simple systems (such as pH meters and balances) may only require calibration, whereas complex systems require ‘validation for intended purpose’. Validation effort increases from left to right in the diagram. However, it is common for companies to overlook systems of apparent lower complexity. Within these systems it may be possible to manipulate data or repeat testing to achieve a desired outcome with limited opportunity for detection (e.g. stand-alone systems with a user configurable output such as ECG machines, FTIR, UV spectrophotometers).

90

Different data has varying importance to quality, safety and efficacy decisions. Data criticality may be determined by considering the type of decision influenced by the data. Data risk reflects its vulnerability to unauthorised deletion or amendment, and the opportunity for detection during routine review.

95

Reduced effort and/or frequency of control measures may be justified for data that has a lesser impact to product and patient, if those data are obtained from a process that does not provide the opportunity for amendment without specialist software/knowledge

99

Data risk is typically increased by complex, inconsistent processes, with open ended and subjective outcomes compared to simple tasks that are consistent, well defined and objective.

100  
101

Automation, or the use of a ‘validated system’ (e.g. e-CRF; analytical equipment) may not be low risk in terms of data integrity if the validated system is considered in isolation of the relevant business

102  
103



104 process (trial subject data entry, analytical sample preparation). Where there is human intervention,  
105 particularly influencing how or what data is recorded or reported, there may be increased risk from  
106 poor organisational controls or data verification due to overreliance on the system's validated state.

107 Companies should balance data risk with other quality and compliance priorities. Prioritisation of  
108 actions, including acceptance of an appropriate level of residual risk should be documented,  
109 communicated to senior management, and kept under review. In situations where long-term  
110 remediation actions are identified, risk reducing short-term measures should be implemented to  
111 provide acceptable data governance in the interim.

### 112 **Designing systems to assure data quality and integrity**

113 Systems and processes should be designed in a way that encourages compliance with the principles  
114 of data integrity. Consideration should be given to ease of access, usability and location whilst  
115 ensuring appropriate control of the activity guided by the criticality of the data. Examples include:  
116

- 117 • Access to appropriately controlled / synchronised clocks for recording timed events.
- 118 • Accessibility of records at locations where activities take place so that ad hoc data recording and  
119 later transcription to official records is not necessary
- 120 • 'Free access' to blank paper proformae for raw/source data recording should be controlled  
121 where this is appropriate. Reconciliation may be necessary to prevent recreation of a record.
- 122 • User access rights that prevent (or audit trail) unauthorised data amendments
- 123 • Automated data capture or printers attached to equipment such as balances
- 124 • Control of physical parameters (time, space, equipment) that permit performance of tasks and  
125 recording of data as required.
- 126 • Access to raw data for staff performing data checking activities.
- 127
- 128

129 The use of scribes to record activity on behalf of another operator should be considered 'exceptional',  
130 and only take place where:

- 131 • The act of contemporaneous recording compromises the product or activity e.g. documenting  
132 line interventions by sterile operators.
- 133 • To accommodate cultural or staff literacy/language limitations, for instance where an activity is  
134 performed by an operator, but witnessed and recorded by a Supervisor or Officer.
- 135
- 136
- 137

138 In both situations, the supervisory recording should be contemporaneous with the task being  
139 performed, and should identify both the person performing the task and the person completing the  
140 record. The person performing the task should countersign the record wherever possible, although it  
141 is accepted that this countersigning step will be retrospective. The process for supervisory (scribe)  
142 documentation completion should be described in an approved procedure, which should also specify  
143 the activities to which the process applies.



147 **Definitions and guidance**

148  
149 In the following section, definitions are given in italic text.

150  
151 **1. Data**

152  
153 *Facts and statistics collected together for reference or analysis*

154  
155 Data should be:

- 156  
157 A - attributable to the person generating the data  
158 L – legible and permanent  
159 C – contemporaneous  
160 O – original record (or true copy)  
161 A - accurate  
162

163 Data governance measures should also ensure that data is complete, consistent and enduring  
164 throughout the lifecycle

165  
166  
167 **2. Raw data (GCP: synonymous with ‘source data’)**

168  
169 *Original records, retained in the format in which they were originally generated (i.e. paper or*  
170 *electronic), or as a ‘true copy’. Raw data must be contemporaneously and accurately recorded by*  
171 *permanent means.*

172  
173 The definition of ‘original records’ currently varies across regulatory documents. By its nature, paper  
174 copies of raw data generated electronically cannot be considered as ‘raw data’.

175  
176 Raw data must permit the full reconstruction of the activities resulting in the generation of the data. In  
177 the case of basic electronic equipment which does not store electronic data, or provides only a printed  
178 data output (e.g. balance or pH meter), the printout constitutes the raw data.

179  
180 In the following definitions, the term ‘data’ includes raw data.

181  
182  
183 **3. Metadata:**

184  
185 *Metadata is data that describe the attributes of other data, and provide context and meaning.*  
186 *Typically, these are data that describe the structure, data elements, inter-relationships and other*  
187 *characteristics of data. It also permits data to be attributable to an individual (or if automatically*  
188 *generated, to the original data source).*

189  
190 Metadata forms an integral part of the original record. Without metadata, the data has no meaning.

191  
192 See also ‘flat files’  
193  
194  
195



196 Example (i) **3.5**

197  
198 metadata, giving context and meaning, (*italic text*) are:

199  
200 *sodium chloride batch 1234, 3.5mg. J Smith 01/07/14*

201  
202  
203 Example (ii) **3.5**

204  
205 metadata, giving context and meaning, (*italic text*) are:

206  
207 *Trial subject A123, sample ref X789 taken 30/06/14 at 1456hrs.*  
208 *INR, 3.5mg. Analyst: J Smith 01/07/14*

209  
210  
211 **4. Data Integrity**

212  
213  
214 *The extent to which all data are complete, consistent and accurate throughout the data lifecycle.*

215  
216 Data integrity arrangements must ensure that the accuracy, completeness, content and meaning of  
217 data is retained throughout the data lifecycle.

218  
219  
220 **5. Data Governance**

221  
222  
223 *The sum total of arrangements to ensure that data, irrespective of the format in which it is generated,*  
224 *is recorded, processed, retained and used to ensure a complete, consistent and accurate record*  
225 *throughout the data lifecycle.*

226  
227 Data governance should address data ownership throughout the lifecycle, and consider the design,  
228 operation and monitoring of processes / systems in order to comply with the principles of data integrity  
229 including control over intentional and unintentional changes to information.

230  
231 Data Governance systems should include staff training in the importance of data integrity principles  
232 and the creation of a working environment that enables visibility of errors, omissions and aberrant  
233 results.

234  
235 Senior management is responsible for the implementation of systems and procedures to minimise the  
236 potential risk to data integrity, and for identifying the residual risk, using risk management techniques  
237 such as the principles of ICH Q9. Contract Givers should ensure that data ownership, governance  
238 and accessibility are included in a contract/technical agreement. The Contract Giver should also  
239 perform a data governance review as part of their vendor assurance programme.

240  
241 Routine data review should evaluate the integrity of an individual data set, compliance with  
242 established organisational and technical measures and any data risk indicators (e.g. data  
243 amendment). Periodic review of data governance measures (for example audit) should assess



244 effectiveness of established organisational and technical measures, and also consider the possibility  
245 of unauthorised activity.

246  
247 Data governance systems should also ensure that data are readily available and directly accessible  
248 on request from national competent authorities.

## 249 250 251 **6. Data Lifecycle**

252  
253 *All phases in the life of the data (including raw data) from initial generation and recording through*  
254 *processing (including analysis, transformation or migration), use, data retention, archive / retrieval and*  
255 *destruction.*

256  
257 The procedures for destruction of data should consider data criticality and where applicable legislative  
258 retention requirements. Archival arrangements should be in place for long term retention of relevant  
259 data in compliance with legislation.

## 260 261 262 263 **7. Data transfer / migration**

264  
265 Data transfer is the process of transferring data and metadata between storage media types or  
266 computer systems. Data migration changes the format of data to make it usable or visible on an  
267 alternative computerised system.

268  
269 Data transfer/migration should be designed and validated to ensure that data integrity principles are  
270 maintained.

## 271 272 273 **8. Data Processing**

274  
275 *A sequence of operations performed on data in order to extract, present or obtain information in a*  
276 *defined format. Examples might include: statistical analysis of individual patient data to present*  
277 *trends or conversion of a raw electronic signal to a chromatogram and subsequently a calculated*  
278 *numerical result*

279  
280 There should be adequate traceability of any user defined parameters used within data processing  
281 activities. Audit trails and retained records should allow reconstruction of all data processing activities  
282 regardless of whether the output of that processing is subsequently reported or otherwise used. If  
283 data processing has been repeated with progressive modification of processing parameters this  
284 should be visible to ensure that the processing parameters are not being manipulated to achieve a  
285 more desirable end point.

## 286 287 288 289 290 291 **9. Recording data:** 292



293 Companies should have an appropriate level of process understanding and technical knowledge of  
294 systems used for data recording, including their capabilities, limitations and vulnerabilities.  
295

296 The selected method should ensure that data of appropriate accuracy, completeness, content and  
297 meaning is collected and retained for its intended use. Where the capability of the electronic system  
298 permits dynamic storage it is not appropriate for low-resolution or static (printed / manual) data to be  
299 collected in preference to high resolution or dynamic (electronic) data.  
300

## 301 302 **10. Excluding Data:**

303  
304 Data may only be excluded where it can be demonstrated through sound science that the data is  
305 anomalous or non-representative. In all cases, this justification should be documented and considered  
306 during data review and reporting. All data (even if excluded) should be retained with the original data  
307 set, and be available for review in a format that allows the validity of the decision to exclude the data  
308 to be confirmed.  
309

## 310 311 **11. Original record / True Copy(also referred to as ‘certified copy’ or ‘verified copy’):**

### 312 313 **11.1. Original record:**

314  
315 *Data as the file or format in which it was originally generated, preserving the integrity (accuracy,*  
316 *completeness, content and meaning) of the record, e.g. original paper record of manual observation,*  
317 *or electronic raw data file from a computerised system*  
318

319 Data may be static (e.g. a ‘fixed’ record such as paper or pdf) or dynamic (e.g. an electronic record  
320 which the user/reviewer can interact with). An analogy being a group of still images (photographs –  
321 the static ‘paper copy’ example) may not provide the full content and meaning of the same event as a  
322 recorded moving image (video – the dynamic ‘electronic record’ example).  
323

324 Example 1: An electronic monitoring system records temperatures every 5 minutes, providing the  
325 ability to interrogate data to investigate excursions (magnitude and duration). This ability is  
326 compromised when working from a summary graph.  
327

328 Example 2: Chromatography systems provide dynamic electronic records in database format with the  
329 ability to track, trend, and query data. This allows the reviewer (with proper access permissions) to  
330 interact with the data (e.g. view hidden fields, and expand the baseline) to view the integration more  
331 clearly. Once printed or converted to static file format (e.g. .pdfs), chromatography records lose the  
332 interaction capability.  
333

### 334 335 **11.2. True Copy:**

336 *A copy of original information that been verified as an exact (accurate and complete) copy having all*  
337 *of the same attributes and information as the original. The copy may be verified by dated signature or*  
338 *by a validated electronic signature. A true copy may be retained in a different electronic file format to*  
339 *the original record, if required, but must retain the equivalent static/dynamic nature of the original*  
340 *record.*  
341





342 Original records and true copies must preserve the integrity (accuracy, completeness, content and  
343 meaning) of the record. True copies of original records may be retained in place of the original record  
344 (e.g. scan of a paper record), provided that a documented system is in place to verify and record the  
345 integrity of the copy. Companies should consider any risk associated with the destruction of original  
346 records.

347  
348 It should be possible to create a true copy of electronic data, including relevant metadata, for the  
349 purposes of review, backup and archival. Accurate and complete copies for certification should  
350 include the meaning of the data (e.g. date formats, context, layout, electronic signature and  
351 authorisations), as well as the full audit trail. Consideration should be given to the dynamic  
352 functionality of a 'true copy' throughout the retention period (see 'archive').  
353

354 Where certified copies are made, the process for certification should be described, including the  
355 process for ensuring that the copy is complete and accurate and for identifying the certifying party and  
356 their authority for making that copy. The process of making a true copy of electronic data should be  
357 validated.  
358

359 Data must be retained in a dynamic form where this is critical to its integrity or later verification. It is  
360 conceivable for some data generated by electronic means to be retained in an acceptable paper or  
361 pdf format, where it can be justified that a static record maintains the integrity of the original data.  
362 However, the data retention process must be shown to include verified copies of all raw data,  
363 metadata, relevant audit trail and result files, any variable software/system configuration settings  
364 specific to each record, and all data processing runs (including methods and audit trails) necessary  
365 for reconstruction of a given raw data set. It would also require a documented means to verify that  
366 the printed records were an accurate representation. This approach is likely to be onerous in its  
367 administration to enable a GxP compliant record.  
368

## 369 **12. Computer system transactions:**

370  
371  
372 *A computer system transaction is a single operation or sequence of operations performed as a single*  
373 *logical 'unit of work'. The operation(s) that make up a transaction may not be saved as a permanent*  
374 *record on durable storage until the user commits the transaction through a deliberate act (e.g.*  
375 *pressing a save button), or until the system forces the saving of data.*  
376

377 The metadata (i.e., user name, date, and time) is not captured in the system audit trail until the user  
378 saves the transaction to durable storage. In computerised systems, an electronic signature may be  
379 required in order for the record to be saved and become permanent.  
380

381 Computer systems should be designed to ensure that the execution of critical steps are recorded  
382 contemporaneously by the user and are not combined into a single computer system transaction with  
383 other operations. A critical step is a parameter that must be within an appropriate limit, range, or  
384 distribution to ensure the safety of the subject or quality of the product or data.  
385

386 Computerised systems should enforce saving immediately after critical data entry. Data entry prior to  
387 saving to permanent memory with audit trail (server, database) is considered to be temporary  
388 memory. These data are at risk of amendment or deletion without audit trail visibility. The length of  
389 time that data is held in temporary memory should be minimised.  
390



391 Critical steps should be documented with process controls that consider system design (prevention),  
392 together with monitoring and review processes (surveillance). Surveillance activities should alert to  
393 failures that are not addressed by the process design.  
394

395 Example:

396 Computerised system may be configured to prevent data manipulation (prevention). This does not  
397 restrict a person from repeating the process by manipulating data to achieve a desired result. Periodic  
398 reviews (surveillance) for undisclosed data may reduce risk from repeated events.  
399

### 400 401 **13. Audit Trail**

402  
403 *Audit trails are metadata that are a record of critical information (for example the change or deletion of*  
404 *relevant data) that permit the reconstruction of activities.*  
405

406 Where computerised systems are used to capture, process, report, store and archive raw data  
407 electronically, system design should always provide for the retention of audit trails to show all  
408 changes to the data while retaining previous and original data. It should be possible to associate all  
409 changes to data with the persons making those changes, and changes should be time stamped and a  
410 reason given. The items included in the audit trail should be those of relevance to permit  
411 reconstruction of the process or activity.  
412

413 Audit trails should be switched on. Users (with the exception of system administrator) should not have  
414 the ability to amend or switch off the audit trail.  
415

416 The relevance of data retained in audit trails should be considered by the company to permit robust  
417 data review / verification. It is not necessary for audit trail review to include every system activity (e.g.  
418 user log on/off, keystrokes etc.) and may be achieved by review of appropriately designed and  
419 validated system reports.  
420

421 Where relevant audit trail functionality does not exist (e.g. within legacy systems and spreadsheets)  
422 an equivalent level of control may be achieved for example by the use of log books, protecting each  
423 version and change control.  
424

425 Routine data review should include a documented audit trail review. When designing a system for  
426 review of audit trails, this may be limited to those with GxP relevance (e.g. relating to data creation,  
427 processing, modification and deletion etc). Audit trails may be reviewed as a list of relevant data, or by  
428 a 'exception reporting' process. An exception report is a validated search tool that identifies and  
429 documents predetermined 'abnormal' data or actions, which requires further attention or investigation  
430 by the data reviewer.

431 QA should have sufficient knowledge and system access to review relevant audit trails, raw data and  
432 metadata as part of audits to ensure on-going compliance with the company's data governance policy  
433 and regulatory requirements. See also 'data governance'.  
434

435 If no audit trailed system exists a paper based audit trail to demonstrate changes to data will be  
436 permitted until a fully audit trailed (integrated system or independent audit software using a validated  
437 interface) system becomes available. These hybrid systems are acceptable, where they achieve  
438 equivalence to integrated audit trail, such as described in Chapter 4 of the GMP Guide. If such



439 equivalence cannot be demonstrated, it is expected that GMP facilities should upgrade to an audit  
440 trailed system by the end of 2017 (reference: Art 23 of Directive 2001/83/EC).

#### 443 **14. Electronic signatures**

444 The use of electronic signatures should be compliant with the requirements of international standards  
445 such as Directive 1999/93/EC (requirements relevant to 'advanced electronic signature').

446 Where a paper or pdf copy of an electronically signed document is produced the metadata associated  
447 with an electronic signature should be maintained together with the associated document.

448 An inserted image of a signature alone, or a footnote indicating that the document has been  
449 electronically signed (where this has been entered by a means other than the validated electronic  
450 signature process) is not sufficient.

#### 456 **15. Data Review**

457 There should be a procedure that describes the process for the review and approval of data. Data  
458 review should also include a review of relevant metadata, including audit trails.

459 Review should be based upon original data or a true copy. Summary reports of data are often  
460 supplied between companies (contract givers and acceptors). However, it must be acknowledged that  
461 summary reports are limited, in that critical supporting data and metadata are often not included.

462 Prior to acceptance of summary reports, a risk-based evaluation of the contract acceptor's quality  
463 system including compliance with data integrity principles should be established.

464 Where data review is not conducted by the company that generated the data, the responsibilities for  
465 data review must be documented and agreed by both parties.

466 Data review should be documented.

467 A procedure should describe the actions to be taken if data review identifies an error or omission. This  
468 procedure should enable data corrections or clarifications to be made in a GxP compliant manner,  
469 providing visibility of the original record, and audit trailed traceability of the correction, using ALCOA  
470 principles (see 'data' definition).

#### 479 **16. Computerised system user access / system administrator roles**

480 Full use should be made of access controls to ensure that people have access only to functionality  
481 that is appropriate for their job role, and that actions are attributable to a specific individual.

482 Companies must be able to demonstrate the access levels granted to individual staff members and  
483 ensure that historical information regarding user access level is available. Controls should be applied  
484 at both the operating system and application levels.



487 Shared logins or generic user access should not be used. Where the computerised system design  
488 supports individual user access, this function must be used. This may require the purchase of  
489 additional licences.

490  
491 It is acknowledged that some computerised systems support only a single user login or limited  
492 numbers of user logins. Where no suitable alternative computerised system is available, equivalent  
493 control may be provided by third party software, or a paper based method of providing traceability  
494 (with version control). The suitability of alternative systems should be justified and documented.  
495 Increased data review is likely to be required for hybrid systems because they are vulnerable to non-  
496 attributable data changes. It is expected that companies should be implementing systems which  
497 comply with current regulatory expectations. It is expected that GMP facilities should upgrade to  
498 system with individual login and audit trails by the end of 2017 (reference: Art 23 of Directive  
499 2001/83/EC).

500  
501 System administrator access should be restricted to the minimum number of people possible taking  
502 account of the size and nature of the company. The generic system administrator account should not  
503 be available for use. Personnel with system administrator access should log in with unique credentials  
504 that allow actions in the audit trail(s) to be attributed to a specific individual.

505  
506 System Administrator rights (permitting activities such as data deletion, database amendment or  
507 system configuration changes) should not be assigned to individuals with a direct interest in the data  
508 (data generation, data review or approval). Where this is unavoidable in the company structure, a  
509 similar level of control may be achieved by the use of dual user accounts with different privileges. All  
510 changes performed under system administrator access should be visible to, and approved within, the  
511 quality system.

512  
513 The individual should log in using the account with the appropriate access rights for the given task  
514 e.g. a laboratory manager performing data checking should not log in as system administrator where  
515 a more appropriate level of access exists for that task.

516  
517 Individuals may require changes in their access rights depending on the status of clinical trial data.  
518 For example, once data management processes are complete the data is 'locked' by removing editing  
519 access rights. This should be able to be demonstrated within the system.

## 520 521 522 **17. Data retention**

523  
524 Data retention may be classified as either archive (protected data for long term storage) or backup  
525 (dynamic data for the purposes of disaster recovery).

526  
527 Data and document retention arrangements should ensure the protection of records from deliberate or  
528 inadvertent alteration or loss. Secure controls must be in place to ensure the data integrity of the  
529 record throughout the retention period, and validated where appropriate. See also data transfer /  
530 migration.

531  
532 Data (or a true copy thereof) generated in paper format may be retained for example by scanning,  
533 provided that there is a process in place to ensure that the copy is certified.

### 534 535 **17.1. Archive**



536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

*A designated secure area or facility (e.g. cabinet, room, building or computerised system) for the long term, permanent retention of complete data and relevant metadata in its final form for the purposes of reconstruction of the process or activity.*

Archive records may be the original data or a 'true copy', and should be protected such that they cannot be altered or deleted without detection.

The archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period. In the case of electronic data archival, this process should be validated, and in the case of legacy systems the ability to review data periodically verified (i.e. to confirm the continued support of legacy computerised systems).

When legacy systems can no longer be supported, consideration should be given to maintaining the software for data accessibility purposes as long as reasonably practicable. This may be achieved by maintaining software in a virtual environment (e.g. Cloud or SaaS). Migration to an alternative file format which retains the 'true copy' attributes of the data may be necessary with increasing age of the legacy data. The migration file format should be selected taking into account the balance of risk between long term accessibility versus possibility of reduced dynamic data functionality (e.g. data interrogation, trending, re-processing etc).

## **17.2. Backup**

*A copy of current (editable) data, metadata and system configuration settings (variable settings which relate to a record or analytical run) maintained for the purpose of disaster recovery.*

Backup and recovery processes should be validated and periodically tested.

## **18. File structure**

### **18.1. Flat files:**

*A 'flat file' is an individual record which may not carry any additional metadata with it, other than that included in the file itself*

Flat files may carry basic metadata relating to file creation and date of last amendment, but may not audit trail the type and sequence of amendments. When creating flat file reports from electronic [data](#), the metadata and audit trails relating to the generation of the raw data may be lost, unless these are retained as a 'true copy'.

Consideration also needs to be given to the 'dynamic' nature of the data, where appropriate (see 'true copy' definition).

There is an inherently greater data integrity risk with flat files when compared to data contained within a relational database in that they are easier to manipulate and delete as a single file.

### **18.2. Relational database:**



585 *A relational database stores different components of associated data and metadata in different*  
586 *places. Each individual record is created and retrieved by compiling the data and metadata for review*  
587 *using a database reporting tool.*  
588

589 This file structure is inherently more secure, as the data is held in a large file format which preserves  
590 the relationship between data and metadata.

591 This is more resilient to attempts to selectively delete, amend or recreate data and the metadata trail  
592 of actions, compared to a flat file system.

593 Retrieval of information from a relational database requires a database reporting tool, or the original  
594 application which created the record.

595 Access rights for database entry or amendment should be controlled, and consistent with the  
596 requirements for computerised system user access / system administrator roles.

600

601

## 602 **19. Validation - for intended purpose (See also GMP Annex 15 and GAMP 5)**

603

604

605 Computerised systems should comply with regulatory requirements and associated guidance and be  
606 validated for their intended purpose. This requires an understanding of the computerised system's  
607 function within a process. For this reason, the acceptance of vendor-supplied validation data in  
608 isolation of system configuration and intended use is not acceptable. In isolation from the intended  
609 process or end user IT infrastructure, vendor testing is likely to be limited to functional verification  
610 only, and may not fulfil the requirements for performance qualification.

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

## **20. Cloud providers and virtual service / platforms (also referred to as software as a service SaaS / platform as a service (PaaS) / infrastructure as a service (IaaS))**

Where 'cloud' or 'virtual' services are used, particular attention should be paid to understanding the  
service provided, ownership, retrieval, retention and security of data.

The physical location where the data is held, including impact of any laws applicable to that  
geographic location should be considered. The responsibilities of the contract giver and acceptor  
should be defined in a technical agreement or contract. This should ensure timely access to data  
(including metadata and audit trails) to the data owner and national competent authorities upon  
request. Contracts with providers should define responsibilities for archiving and continued readability  
of the data throughout the retention period (see archive). 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.

Business continuity arrangements should be included in the contract, and tested.