



1  
2  
3 DRAFT WORKING DOCUMENT FOR COMMENTS:  
4

5 Guideline on data integrity  
6  
7  
8

Please send your comments to **Dr Sabine Kopp**, Team Lead, Norms and Standards for Pharmaceuticals, Technical Standards and Specifications ([kopps@who.int](mailto:kopps@who.int)), with a copy to Ms Claire Vogel ([vogelc@who.int](mailto:vogelc@who.int)) before 15 August 2020. Please use our attached Comments Table for this purpose.

Our working documents are sent out electronically and they will also be placed on the WHO Medicines website ([http://www.who.int/medicines/areas/quality\\_safety/quality\\_assurance/guidelines/en/](http://www.who.int/medicines/areas/quality_safety/quality_assurance/guidelines/en/)) for comments under the "Current projects" link. If you wish to receive all our draft guidelines, please send your email address to [jonessi@who.int](mailto:jonessi@who.int) and your name will be added to our electronic mailing list.

9  
10  
11  
12  
13 © World Health Organization 2020  
14

15 All rights reserved.  
16

17 *This draft is intended for a restricted audience only, i.e. the individuals and organizations having received this draft. The draft may not be reviewed, abstracted, quoted, reproduced, transmitted, distributed, translated or adapted, in part or in whole, in any form or by any means outside these individuals and organizations (including the organizations' concerned staff and member organizations) without the permission of the World Health Organization. The draft should not be displayed on any website.*  
18  
19  
20

21  
22 *Please send any request for permission to: Dr Sabine Kopp, Group Lead, Norms and Standards for Pharmaceuticals, Department of Access to Medicines and Health Products, World Health Organization, CH-1211 Geneva 27, Switzerland, email: [kopps@who.int](mailto:kopps@who.int).*  
23  
24  
25

26 *The designations employed and the presentation of the material in this draft do not imply the expression of any opinion whatsoever on the part of the World Health Organization concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted lines on maps represent approximate border lines for which there may not yet be full agreement.*  
27  
28  
29

30  
31 *The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by the World Health Organization in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.*  
32  
33  
34

35 *All reasonable precautions have been taken by the World Health Organization to verify the information contained in this draft. However, the printed material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the World Health Organization be liable for damages arising from its use.*  
36  
37  
38  
39

40 *This draft does not necessarily represent the decisions or the stated policy of the World Health Organization.*  
41

SCHEDULE FOR DRAFT WORKING DOCUMENT QAS/19.819/Rev.1

[*Note from Secretariat:* in view of COVID-19, the schedule had to be adapted as face-to-face meetings were postponed and/or replaced by virtual meetings]

## Guideline on data integrity

Description of activity	Date
Preparation of the document following recommendation of the Fifty-fourth WHO Expert Committee on Specifications for Pharmaceutical Preparations (ECSP).	October 2019
Mailing of working document inviting comments, including to the Expert Advisory Panel on the International Pharmacopoeia and Pharmaceutical Preparations (EAP), and posting of the working document on the WHO website for public consultation.	November 2019–January 2020
Consolidation of comments received and review of feedback. Preparation of working document for discussion.	March – May 2019
Discussion of working document and feedback received during the public consultation and the informal Consultation on Good Practices for Health Products Manufacture and Inspection. In view of the logistical situation with regard to COVID-19, the consultation was replaced by virtual meetings of a working group composed of inspectors from Brazil, China, India, Italy and South Africa, as well as UNICEF.	10 and 12 June 2020
Mailing of the revised working document inviting comments, including to the EAP, and posting the working document on the WHO website for the second round of public consultation.	June 2020
Consolidation of comments received and review of feedback. Preparation of working document for discussion.	September 2020
Presentation to the Fifty-fifth ECSP meeting.	12-16 October 2020
Any other follow-up action as required.	

48

49

## Guideline on data integrity

50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74

This document will replace the WHO *Guidance on good data and record management practices* (Annex 5, WHO Technical Report Series, No. 996, 2016) (1).

1. Introduction and background
  2. Scope
  3. Glossary
  4. Data governance
  5. Quality risk management
  6. Management review
  7. Outsourcing
  8. Training
  9. Data
  10. Data integrity
  11. Good documentation practices
  12. Computerized systems
  13. Corrective and preventive actions
- References
- Further reading
- Annex 1: Examples of data integrity management

Draft for comments

## 75 **1. Introduction and background**

76

77 1.1. Data governance and its related measures are important to ensure the reliability of data and  
78 records in good practice (GxP) activities and regulatory submissions. The data and records  
79 should be attributable, legible, contemporaneous, original and accurate, commonly referred to  
80 as “ALCOA+”.

81

82 1.2. In recent years, the number of observations made regarding the integrity of data,  
83 documentation and record management practices during inspections of good manufacturing  
84 practice (GMP) (2), good clinical practice (GCP) and good laboratory practice (GLP) have been  
85 increasing. The possible causes for this may include (i) reliance on inadequate human  
86 practices; (ii) poorly defined procedures; (iii) resource constraints; (iv) the use of computerized  
87 systems that are not capable to meet regulatory requirements or are inappropriately managed  
88 and validated (3,4); (v) inappropriate data flow (e.g. manual data transfer); and (vi) failure to  
89 adequately review and manage original data and records.

90

91 1.3. Data governance control strategies using quality risk management principles (5) are required  
92 to mitigate such risks. Examples of controls may include, but are not limited to:

- 93 • the establishment and implementation of a data integrity (DI) policy;
- 94 • the establishment and implementation of procedures that will facilitate compliance  
95 with DI requirements and expectations;
- 96 • the adoption of a quality culture within the company that encourages personnel to be  
97 transparent about failures, which includes a reporting mechanism inclusive of  
98 investigation and follow-up processes;
- 99 • the application of quality risk management (QRM) with the identification of all areas of  
100 risk to DI through data integrity risk assessment (DIRA) and the implementation of  
101 appropriate controls to eliminate or reduce risks to an acceptable level throughout the  
102 life-cycle of the data;
- 103 • ensuring sufficient resources are available to implement and complete a DI program  
104 and to monitor compliance with DI policies and procedures and processes, and to  
105 facilitate continuous improvement of both;

- 106
- 107
- 108
- 109
- 110
- 111
- 112
- 113
- 114
- the provision of necessary training for personnel in, for example, GxP, computerized systems and the principles of DI;
  - the implementation and validation of computerized systems appropriate for their intended use, including all relevant DI requirements in order to ensure that the computerized system has the necessary controls to protect the electronic data (3);
  - the definition and management of the appropriate roles and responsibilities for contract givers and contract acceptors, entered into quality agreements and contracts including a focus on DI requirements.

## 115 2. Scope

116

117 2.1. This guideline provides information, guidance and recommendations to facilitate compliance  
118 with regulatory requirements related to DI documentation and record management.

119

120 2.2. The scope of this guideline is designated as "GxP" for pharmaceutical products. The principles  
121 could also be applicable to vector control products.

122

123 2.3. Where possible, this guideline has been harmonised with other published documents. This  
124 guideline should also be read with other WHO good practices guidelines and publications.

125

126 2.4. The principles of this guideline apply to contract givers and contract acceptors. Contract givers  
127 are ultimately responsible for the integrity of data provided to them by contract acceptors.  
128 Contract givers should therefore ensure that contract acceptors have the appropriate  
129 capabilities and comply with the principles contained in this guideline documented in quality  
130 agreements.

131

## 132 3. Glossary

133

134 The definitions given below apply to the terms used in these guidelines. They may have different  
135 meanings in other contexts.

136

137 **ALCOA+**. A commonly used acronym for “attributable, legible, contemporaneous, original and  
138 accurate” which puts additional emphasis on the attributes of being complete, consistent, enduring  
139 and available throughout the data life cycle for the defined retention period – implicit basic ALCOA  
140 principles.

141  
142 **archiving**. Archiving is the process of protecting records from the possibility of being further altered or  
143 deleted, and storing these records under the control of independent data management personnel  
144 throughout the required retention period. Archived records should include, for example, associated  
145 metadata and electronic signatures.

146  
147 **audit trail**. The audit trail is a form of metadata containing information associated with actions that  
148 relate to the creation, modification or deletion of GxP records. An audit trail provides for a secure  
149 recording of life cycle details such as creation, additions, deletions or alterations of information in a  
150 record, either paper or electronic, without obscuring or overwriting the original record. An audit trail  
151 facilitates the reconstruction of the history of such events relating to the record regardless of its  
152 medium, including the “who, what, when and why” of the action.

153  
154 **certified true copy or true copy**. A copy (irrespective of the type of media used) of the original record  
155 that has been verified (i.e. by a dated signature or by generation through a validated process) to have  
156 the same information, including data that describe the context, content, and structure, as the original.

157  
158 **data**. All original records and true copies of original records, including source data and metadata, and  
159 all subsequent transformations and reports of these data which are generated or recorded at the time  
160 of the GMP activity and which allow full and complete reconstruction and evaluation of the GMP  
161 activity.

162  
163 Data should be accurately recorded by permanent means at the time of the activity. Data may be  
164 contained in paper records (such as worksheets and logbooks), electronic records and audit trails,  
165 photographs, microfilm or microfiche, audio or video files or any other media whereby information  
166 related to GMP activities is recorded

167  
168 **data governance**. The sum total of arrangements which provide assurance of data quality. These  
169 arrangements ensure that data, irrespective of the process, format or technology in which it is

170 generated, recorded, processed, retained, retrieved and used will ensure an attributable, legible,  
171 contemporaneous, original, accurate, complete, consistent, enduring and available record throughout  
172 the data life cycle.

173

174 **data life cycle.** All phases of the process by which data are created, recorded, processed, reviewed,  
175 analysed and reported, transferred, stored and retrieved and monitored, until retirement and disposal.  
176 There should be a planned approach to assessing, monitoring and managing the data and the risks to  
177 those data, in a manner commensurate with the potential impact on patient safety, product quality  
178 and/or the reliability of the decisions made throughout all phases of the data life cycle.

179

180 **electronic signatures.** A signature in digital form (bio-metric or non-biometric) that represents the  
181 signatory. In legal terms, it is the equivalent of the handwritten signature of the signatory.

182

183 **good practices (GxP).** An acronym for the group of good practice guides governing the preclinical,  
184 clinical, manufacturing, testing, storage, distribution and post-market activities for regulated  
185 pharmaceuticals, biologicals and medical devices, such as GLP, GCP, GMP, good pharmacovigilance  
186 practices (GVP) and good distribution practices (GDP).

187

188 **metadata.** Metadata are data about data that provide the contextual information required to  
189 understand those data. These include structural and descriptive metadata. Such data describe the  
190 structure, data elements, interrelationships and other characteristics of data. They also permit data to  
191 be attributable to an individual. Metadata necessary to evaluate the meaning of data should be  
192 securely linked to the data and subject to adequate review. For example, in weighing, the number 8 is  
193 meaningless without metadata, such as, the unit, milligram, gram, kilogram, and so on. Other examples  
194 of metadata include the time/date stamp of an activity, the operator identification (ID) of the person  
195 who performed an activity, the instrument ID used, processing parameters, sequence files, audit trails  
196 and other data required to understand data and reconstruct activities.

197

198 **raw data.** The original record (data) which can be described as the first-capture of information, whether  
199 recorded on paper or electronically. Raw data is synonymous with source data).

200

201

202

## 203 **4. Data governance**

204

205 4.1. Senior management is responsible for the establishment, implementation and control of an  
206 effective quality system and a data governance system by assuring that policies, training and  
207 technical systems are in place.

208

209 4.2. Senior management is responsible for providing the environment to establish, maintain and  
210 continually improve the quality culture, supporting the transparent and open reporting of  
211 deviations, errors or omissions at all levels of the organization.

212

213 4.3. Senior management should be accountable for the implementation of systems and procedures  
214 in order to minimise the potential risk to DI, and to identify the residual risk using risk  
215 management techniques such as the principles of the guidance on quality risk management  
216 from WHO (5) and The International Council for Harmonisation of Technical Requirements for  
217 Pharmaceuticals for Human Use (ICH) (6).

218

219 4.4. There should be a written DI policy.

220

221 4.5. Data should be attributable, legible, contemporaneous, original, accurate, complete,  
222 consistent, enduring and available. This is generally referred to as ALCOA+.

223

224 4.6. The quality system, including documentation such as procedures and formats for recording  
225 data, should be appropriately designed and implemented in order to provide assurance that  
226 records and data meet the principles contained in this guideline.

227

228 4.7. Data governance should address the data roles, responsibilities and accountability throughout  
229 the life cycle and consider the design, operation and monitoring of processes/systems to  
230 comply with the principles of DI, including control over intentional and unintentional changes  
231 to data.

232

233 4.8. Data governance systems should include e.g.:

234

- training in the importance of DI principles;



- 235 • the creation of an appropriate working environment;
- 236 • active encouragement of collecting feedback and continuous improvement; and
- 237 • the reporting of errors, unauthorized changes, omissions and undesirable results.

238

239 4.9. The data governance programme should include policies and procedures addressing data  
240 management. Elements of effective management governance should at least include:

- 241 • management oversight and commitment;
- 242 • the application of QRM;
- 243 • quality metrics and performance indicators;
- 244 • validation;
- 245 • change, incident and deviation management;
- 246 • security, cybersecurity, access and configuration control;
- 247 • database build, data collection, data review, blinded data, randomization;
- 248 • the tracking, trending, reporting of DI anomalies, and lapses or failures for further  
249 action;
- 250 • the prevention of commercial, political, financial and other organizational pressures;
- 251 • adequate resources, systems;
- 252 • workload and facilities to facilitate the right environment that supports DI and effective  
253 controls;
- 254 • monitoring;
- 255 • record-keeping;
- 256 • training; and
- 257 • awareness of the importance of DI, product quality and patient safety.

258

259 4.10. There should be a system for the regular review of documents and data for consistency with  
260 ALCOA+ principles. This includes paper records and electronic records in day-to-day work,  
261 system and facility audits and self-inspections.

262

263 4.11. The effort and resources applied to assure the integrity of the data should be commensurate  
264 with the risk and impact of a DI failure.

265

266 4.12. Where DI weaknesses are identified, the appropriate corrective and preventive actions (CAPA)  
267 should be implemented across all relevant activities and systems and not in isolation.

268 4.13. Significant DI lapses identified that may impact patient safety, product quality or efficacy,  
269 should be reported to the relevant medicine regulatory authorities.

270

271 4.14. Changing from automated or computerised systems to paper-based manual systems or vice-  
272 versa will not in itself remove the need for appropriate DI controls.

273

274 4.15. Good documentation practices should be followed in order to ensure that all records are  
275 complete and in accordance with ALCOA+ principles.

276

277 4.16. Records (paper and electronic) should be kept in a manner that ensures compliance with the  
278 principles of this guideline. These include but are not limited to:

- 279 • restricting the ability to change dates and times for recording events;
- 280 • using controlled documents and forms for recording GxP data;
- 281 • controlling the issuance of blank paper templates for data recording of GxP activities,  
282 with reconciliation and authenticity controls where required;
- 283 • defining access and privilege rights to automated systems, ensuring segregation of  
284 duties;
- 285 • enabling audit trails and restricting the ability to enable or disable audit trails;
- 286 • having automated data capture systems and printers connected to equipment and  
287 instruments in production and quality control where possible;
- 288 • ensuring the proximity of printers to sites of relevant activities;
- 289 • design processes in a way to avoid the unnecessary transcription of data or  
290 unnecessary conversion from paper to electronic and vice versa; and
- 291 • ensuring access to original electronic data and metadata for personnel responsible for  
292 reviewing and checking data.

293

294 4.17. Systems, procedures and methodology used to record and store data should be periodically  
295 reviewed for effectiveness and updated, as necessary, in relation to new technology.

296

297

298

299

## 300 5. Quality risk management

301

302 5.1. The DIRA should be documented. This should cover systems and processes that produce data  
303 or, where data are obtained, data criticality and inherent risks.

304

305 5.2. The risk assessment should evaluate, for example, the relevant GxP computerised systems,  
306 supporting personnel, training, quality systems and extent of outsourced activities.

307

308 5.3. DI risks should be assessed, mitigated, communicated and reviewed throughout the document  
309 and data life cycle at a frequency based on the risk level, as determined by the risk assessment  
310 process.

311

312 5.4. Where the DIRA has highlighted areas for remediation, the prioritisation of actions (including  
313 the acceptance of an appropriate level of residual risk) and the prioritisation of controls should  
314 be documented and communicated. Where long-term remediation actions are identified, risk-  
315 reducing short-term measures should be implemented in order to provide acceptable data  
316 governance in the interim.

317

318 5.5. Controls identified may include organizational, procedural and technical controls such as  
319 procedures, processes, equipment, instruments and other systems in order to both prevent  
320 and detect situations that may impact on DI. Examples include the appropriate content and  
321 design of procedures, formats for recording, access control, the use of computerized systems  
322 and other means.

323

324 5.6. Controls should cover risks to data. Risks to data manipulation include deletion of, changes to,  
325 and exclusion of data or results from data sets without written justification, authorisation  
326 where appropriate, and detection.

327

328 5.7. In line with the current approach in GxP, this guideline recommends a documented risk-based  
329 approach over the life cycle of data considering data criticality. DIRA should be carried out in  
330 order to identify and assess areas of risk.

331

332 5.8. Efficient risk-based controls and the review of data and documents should be identified and  
333 implemented. The effectiveness of the controls should be verified.

334

## 335 **6. Management review**

336

337 6.1. There should be management oversight of quality metrics relevant to data governance.

338

339 6.2. Management should ensure that computerized systems are meeting regulatory requirements  
340 in order to ensure DI compliance and to avoid the acquisition of inadequate systems and  
341 software.

342

343 6.3. The effectiveness of the controls implemented should be measured against the quality metrics  
344 and performance indicators. These should include, for example:

- 345 • the tracking and trending of data;
- 346 • A review of audit trails in, for example, production, quality control, GLP, case report  
347 forms and data processing; and
- 348 • routine audits and/or self-inspections, including DI and computerized systems.

349

## 350 **7. Outsourcing**

351

352 7.1. The outsourcing of activities and responsibilities of each party (contract giver and contract  
353 acceptor) should be clearly described in written agreements. Specific attention should be given  
354 to ensuring compliance with DI requirements.

355

356 7.2. Compliance with the principles and responsibilities should be verified during periodic site  
357 audits. This should include the review of procedures and data (including raw data and  
358 metadata, paper records, electronic data, audit trails and other related data) held by the  
359 contracted organization that are relevant to the contract giver's product or services.

360

361 7.3. Where data and document retention are contracted to a third party, particular attention should  
362 be paid to understanding the transfer, storage and restoration of data held under that  
363 agreement, as well as controls to ensure the integrity of data over their life cycle. This includes

364 data in motion and data at rest. Tools should be identified to ensure data integrity, for example,  
365 encryption.

366

367 7.4. No activity, including outsourcing of databases, should be sub-contracted to a third party  
368 without the prior approval of the contract giver. This should be stated in the contractual  
369 agreements where appropriate.

370

371 7.5. All contracted parties should be aware of the requirements relating to data governance, DI and  
372 data management.

373

## 374 **8. Training**

375

376 8.1. All personnel who interact with GxP data and who perform GxP activities should be trained in  
377 relevant DI principles and abide by organization policies and procedures. This should include  
378 understanding the potential consequences in cases of non-compliance.

379

380 8.2. Personnel should agree to abide by DI principles and should be made aware of the potential  
381 consequences in cases of non-compliance.

382

383 8.3. Personnel should be trained in good documentation practices and measures to prevent and  
384 detect DI issues. Specific training may be required in cases where computerized systems are  
385 used in the generation, processing, interpretation and reporting of data and where risk  
386 assessment has shown that this may be required. Such training should include, for example,  
387 evaluating the system security, back-up, configuration settings and reviewing of electronic data  
388 and metadata, such as audit trails and logs, for individual computerized systems used in the  
389 generation, processing and reporting of data.

390

## 391 **9. Data and data transfer**

392

393 9.1. Data may be recorded manually reflecting an observation, result or other data and information  
394 on paper, or electronically by using equipment and instruments including those linked to

395 computerised systems. A combination of manual and electronic systems may also be used,  
396 referred to as a “hybrid system”.

397

398 9.2. The same considerations for DI apply to data sets such as photographs, videos, DVDs, imagery  
399 and chromatography plates. There should be a documented rationale for the selection of such  
400 a method.

401

402 9.3. Risk-reducing supervisory measures should be implemented where there is difficulty in  
403 accurately and contemporaneously recording data related to critical process parameters or  
404 critical quality attributes.

405

406 9.4. Results and data sets require independent verification if deemed necessary from the DIRA or  
407 by another requirement.

408

409 9.5. Programmes and methods (such as acquisition and processing methods) should ensure that  
410 data meet ALCOA+ principles. Where results or data are processed using a different  
411 method/parameters, then the acquisition method should be recorded. Audit trails with the  
412 required details should allow for reconstruction of all data processing and administrative  
413 activities.

414

415 9.6. Data transfer should not result in any changes to the content or meaning of the data. The  
416 transfer should be tracked in the audit trail or by other suitable means.

417

418 9.7. Data transfer should be validated and computerized interfaces tested, especially systems which  
419 map and or transform data moving between computerized systems.

420

## 421 **10. Good documentation practices**

422

423 10.1. The principles contained in this section are applicable to paper data.

424

425 10.2. Data and recorded media should be durable. Ink should be indelible. Temperature-sensitive  
426 or photosensitive inks and other erasable inks should not be used, or other means should be  
427 identified in order to ensure traceability of the data over their life cycle.

428 10.3. Paper should not be temperature-sensitive, photosensitive or easily oxidizable. If this is not  
429 feasible or limited, then true or certified copies should be available.

430

431 10.4. Specific controls should be implemented in order to ensure the integrity of data and results  
432 recorded on paper records. These may include, but are not limited to:

- 433 • control over the issuance and use of loose paper sheets at the time of recording data;
- 434 • the use of permanent, indelible ink;
- 435 • no use of pencil or erasers;
- 436 • the use of single-line cross-outs to record changes with the identifiable person who  
437 made the change, date and reason recorded (i.e. the paper equivalent to an electronic  
438 audit trail);
- 439 • no use of correction fluid or otherwise, obscuring the original record;
- 440 • controlled issuance of bound, paginated notebooks;
- 441 • controlled issuance of sequentially numbered copies of blank forms with authenticity  
442 controls; and
- 443 • archival of records by designated personnel in secure and controlled archives.

444

## 445 **11. Computerized systems**

446

447 *(Note. This section highlights some specific aspects relating to the use of computerized systems. It is*  
448 *not intended to repeat the information presented in the other WHO guidelines here, such as the WHO*  
449 *Guideline on computerized systems (3), WHO Guideline on validation(2) and WHO Guideline on good*  
450 *chromatography practices (7). See references.)*

451

452 11.1. The computerized system selected should be suitable and validated for its intended use.

453

454 11.2. Where GxP systems are used to acquire, record, transfer, store or process data, management  
455 should have appropriate knowledge of the risks that the system and users may pose to the  
456 integrity of the data.

457

458 11.3. Suitably configured and validated, software should be used where instruments and equipment  
459 with computerised systems are used. The validation should cover the design, implementation

460 and maintenance of controls in order to ensure the integrity of data. The potential for  
461 unauthorized and adverse manipulation of data during the life cycle of the data should be  
462 mitigated and, where possible, eliminated.

463

464 11.4. Where electronic systems with no configurable software and no electronic data retention (e.g.  
465 pH meters, balances and thermometers) are used, controls should be put in place in order to  
466 prevent the adverse manipulation of data and to repeat testing to achieve the desired result.

467

468 11.5. The appropriate controls of detection for lapses in DI principles should be in place. Technical  
469 controls should be used whenever possible. Additional controls should be implemented where  
470 stand-alone systems with a user-configurable output is used, for example, Fourier-transform  
471 infrared spectroscopy (FTIR) and UV spectrophotometers. Examples of detection and  
472 prevention mechanisms may include, but are not limited to, instrument usage logbooks,  
473 electronic audit trails, and external software to lockdown the personal computer workstation.

474

475 11.6. Critical records or data, including metadata, should be reviewed and retained according to risk  
476 assessment. Reduced effort and/or frequency should be justified.

477

## 478 **Access and privileges**

479

480 11.7. There should be a documented system in place that defines the access and privileges of users  
481 of computerized systems. There should be no discrepancy between paper records and  
482 electronic records, including the creation and inactivation of users.

483

484 11.8. Access and privileges should be in accordance with the role and responsibility of the individual  
485 with the appropriate controls to ensure DI (e.g. no modification, deletion or creation of data  
486 outside the allocated responsibility).

487

488 11.9. A limited number of personnel, with no conflict of interest in data, should be appointed as  
489 system administrators. Certain privileges such as data deletion, database amendment or  
490 system configuration changes should not be assigned to administrators without justification -  
491 and such activities should only be done with documented evidence of authorization by another  
492 responsible person. Records should be maintained and audit trails should be enabled in order



493 to track activities of system administrators. Minimally, activity logging for such accounts and  
494 the review of logs by designated roles should be conducted in order to ensure appropriate  
495 oversight.

496

497 11.10. For systems generating, amending or storing GxP data, shared logins or generic user access  
498 should not be used. The computerised system design should support individual user access.  
499 Where a computerised system supports only a single user login or limited numbers of user  
500 logins and no suitable alternative computerised system is available, equivalent control should  
501 be provided by third-party software or a paper-based method that provides traceability (with  
502 version control). The suitability of alternative systems should be justified and documented (8).

503

## 504 **Audit trail**

505

506 11.11. GxP systems should provide for the retention of audit trails. Audit trails should reflect, for  
507 example, users, dates, times, original data and results, changes and reasons for changes.

508

509 11.12. All audit trails should be enabled when software is installed and remain enabled at all times.  
510 There should be evidence of enabling the audit trail. There should be periodical verification  
511 that the audit trail remained enabled throughout the data life cycle.

512

513 11.13. Where a system cannot support ALCOA+ principles by design (e.g. legacy systems with no  
514 audit trail), mitigation measures should be taken for defined temporary periods. For example,  
515 add-on software or paper based controls may be used. The suitability of alternative systems  
516 should be justified and documented. This should be addressed within defined timelines.

517

518 11.14. Routine data review should include a review of audit trails. Evidence of the reviews should  
519 be maintained.

520

## 521 **Electronic signatures**

522

523 11.15. Each electronic signature should be appropriately controlled. An electronic signature should  
524 be:

- 525 • validated;

- 526 • attributable to an individual;
- 527 • free from alteration and manipulation; and
- 528 • date- and time-stamped, where appropriate.

529

530 11.16. An inserted image of a signature or a footnote indicating that the document has been  
531 electronically signed is not adequate unless it was created as part of the validated electronic  
532 signature process. The metadata associated with the signature should be retained.

533

### 534 **Data review and approval**

535

536 11.17. There should be a documented procedure for the routine and periodic review, as well as the  
537 approval of data.

538

539 11.18. A procedure should describe the actions to be taken where errors, discrepancies or omissions  
540 are identified in order to ensure that the appropriate corrective and preventive actions are  
541 taken.

542

543 11.19. A conclusion following the review of original data, metadata and audit trail records should be  
544 documented, signed and dated.

545

### 546 **Data backup, retention and restoration**

547

548 11.20. Data should be retained in such a manner that they are protected, enduring, readily  
549 retrievable and remain readable throughout the records retention period. True copies of  
550 original records may be retained in place of the original record, where justified. Electronic  
551 data should be backed up according to written procedures.

552

553 11.21. Data and records should be kept in a secure area which provides appropriate protection.  
554 Access should be controlled.

555

556 11.22. Retention periods should be defined in authorized procedures.

557

558 11.23. Records reflecting documented reasons for the destruction of data should be maintained.

559 11.24. Backup and restoration processes should be validated. The backup should be done and  
560 periodically restored and verified for completeness and accuracy of data and metadata.  
561 Where any discrepancies are identified, they should be investigated.  
562

## 563 **12. Corrective and preventive actions**

564  
565 12.1. Where organizations use computerized systems (e.g. for GxP data acquisition, processing,  
566 interpretation, reporting) which do not meet current GxP requirements, a workplan towards  
567 upgrading such systems should be documented and implemented in order to ensure  
568 compliance with current GxP.  
569

570 12.2. When GxP lapses in DI are identified, a risk-based approach may be used to determine the  
571 scope of the investigation, root cause, impact and CAPA, as appropriate. Health authorities,  
572 contract givers and other relevant organizations should be notified if the investigation identifies  
573 a significant impact or risk to, for example, materials, products, patients, reported information  
574 or data in application dossiers, and clinical trials.  
575

576

Draft for comments

## 577 **References**

578

579 1. Guidance on good data and record management practices. In: WHO Expert Committee on  
580 Specifications for Pharmaceutical Preparations: fiftieth report. Geneva: World Health  
581 Organization; 2016: Annex 5 (WHO Technical Report Series, No. 996;  
582 [https://www.who.int/medicines/publications/pharmprep/WHO\\_TRS\\_996\\_annex05.pdf?ua=1](https://www.who.int/medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf?ua=1),  
583 accessed 12 June 2020).

584

585 2. Guidelines on good manufacturing practices for pharmaceutical products: main principle. In:  
586 WHO Expert Committee on Specifications for Pharmaceutical Preparations: forty-eighth report.  
587 Geneva: World Health Organization; 2013: Annex 2 (WHO Technical Report Series, No. 986;  
588 [https://www.who.int/medicines/areas/quality\\_safety/quality\\_assurance/TRS986annex2.pdf?](https://www.who.int/medicines/areas/quality_safety/quality_assurance/TRS986annex2.pdf?ua=1)  
589 [ua=1](https://www.who.int/medicines/areas/quality_safety/quality_assurance/TRS986annex2.pdf?ua=1), accessed 4 May 2020).

590

591 3. Good manufacturing practices: guidelines on validation. In: WHO Expert Committee on  
592 Specifications for Pharmaceutical Preparations; fifty-third report. Geneva: World Health  
593 Organization; 2019: Annex 3 (WHO Technical Report Series, No. 1019;  
594 <http://digicollection.org/whogapharm/documents/s23430en/s23430en.pdf>, accessed 5 May  
595 2020).

596

597 4. Good manufacturing practices: guidelines on validation. Appendix 5. Validation of  
598 computerized systems. In: WHO Expert Committee on Specifications for Pharmaceutical  
599 Preparations: fifty-third report. Geneva: World Health Organization; 2019: Annex 3 (WHO  
600 Technical Report Series, No. 1019; [https://www.who.int/medicines/areas/](https://www.who.int/medicines/areas/quality_safety/quality_assurance/WHO_TRS_1019_Annex3.pdf?ua=1)  
601 [quality\\_safety/quality\\_assurance/WHO\\_TRS\\_1019\\_Annex3.pdf?ua=1](https://www.who.int/medicines/areas/quality_safety/quality_assurance/WHO_TRS_1019_Annex3.pdf?ua=1), accessed 4 May 2020).

602

603 5. Guidelines on quality risk management. In: WHO Expert Committee on Specifications for  
604 Pharmaceutical Preparations: forty-seventh report. Geneva: World Health Organization; 2013:  
605 Annex 2 (WHO Technical Report Series, No. 981;  
606 [https://www.who.int/medicines/areas/quality\\_safety/quality\\_assurance/Annex2TRS-981.pdf](https://www.who.int/medicines/areas/quality_safety/quality_assurance/Annex2TRS-981.pdf),  
607 accessed 4 May 2020).

608

- 609 6. ICH harmonised tripartite guideline. Quality risk management Q9. Geneva: International  
610 Conference on Harmonisation of Technical Requirements for Registration of Pharmaceutical  
611 for Human Use; 2005 (<https://database.ich.org/sites/default/files/Q9%20Guideline.pdf>,  
612 accessed 12 June 2020).
- 613
- 614 7. Good chromatography practices. In: WHO Expert Committee on Specifications for  
615 Pharmaceutical Preparations: fifty-fourth report. Geneva: World Health Organization; 2020:  
616 Annex 4 (WHO Technical Report Series, No. 1025;  
617 <https://www.who.int/publications/i/item/978-92-4-000182-4>, accessed 12 June 2020).
- 618
- 619 8. MHRA GxP data integrity guidance and definitions; Revision 1: Medicines & Healthcare  
620 Products Regulatory Agency (MHRA), London, March 2018  
621 ([https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_d  
622 ata/file/687246/MHRA\\_GxP\\_data\\_integrity\\_guide\\_March\\_edited\\_Final.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf), accessed 12 June  
623 2020).
- 624

## 625 Further reading

- 626
- 627 • Data integrity and compliance with CGMP guidance for industry: questions and answers  
628 guidance for industry. U.S. Department of Health and Human Services, Food and Drug  
629 Administration; 2016 ([https://www.fda.gov/files/drugs/published/Data-Integrity-and-  
630 Compliance-With-Current-Good-Manufacturing-Practice-Guidance-for-Industry.pdf](https://www.fda.gov/files/drugs/published/Data-Integrity-and-Compliance-With-Current-Good-Manufacturing-Practice-Guidance-for-Industry.pdf), accessed  
631 15 June 2020).
- 632
- 633 • Good Practices for data management and integrity in regulated GMP/GDP environments.  
634 Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme  
635 (PIC/S), November 2018 (<https://picscheme.org/layout/document.php?id=1567>, accessed 15  
636 June 2020).
- 637
- 638 • Baseline guide Vol 7: risk-based manufacture of pharma products; 2nd edition. ISPE Baseline®  
639 Guide, July 2017. ISPEGAMP® guide: records and data integrity; March 2017.
- 640

- 641 • Data integrity management system for pharmaceutical laboratories PDA Technical Report, No.  
642 80; August 2018.

643

644

645

646

647

Draft for comments

## 648 **Annex 1. Examples in data integrity management**

649

650 This Annex reflects on some examples in data integrity (DI) management in order to support the main  
651 text on DI. It should be noted that these are examples and are intended for the purpose of clarification  
652 only.

653

### 654 **Example 1: Quality risk management and data integrity risk** 655 **assessment**

656

657 Risk management is an important part of good manufacturing practices (GMP). Risks should be  
658 identified and assessed and controls identified and implemented in order to assist manufacturers in  
659 preventing possible DI lapses.

660

661 As an example, a Failure Mode and Effects Analysis (FMEA) model (or any other tool) can be used to  
662 identify and assess the risks relating to any system where data are, for example, acquired, processed,  
663 recorded, saved and archived. The risk assessment can be done as a prospective exercise or  
664 retrospective exercise. Corrective and preventive action (CAPA) should be identified, implemented and  
665 assessed for its effectiveness.

666

667 For example, if during the weighing of a sample, the entry of the date was not contemporaneously  
668 recorded on the worksheet but the date is available on the print-out from a weighing balance and log  
669 book for the balance for that particular activity. The fact that the date was not recorded on the  
670 worksheet may be considered a lapse in data integrity expectations. When assessing the risk relating  
671 to the lack of the date in the data, the risk may be considered different (lower) in this case as opposed  
672 to a situation when there is no other means of traceability for the activity (e.g. no print-out from the  
673 balance). When assessing the risk relating to the lapse in DI, the severity could be classified as “low”  
674 (the data is available on the print-out); it does not happen on a regular basis (occurrence is “low”), and  
675 it could easily be detected by the reviewer (detection is “high”) – therefore the overall risk factor may  
676 be considered low. The root cause as to why the record was not made in the analytical report at the  
677 time of weighing should still be identified and the appropriate action taken to prevent this from  
678 happening again.

679

## 680 **Example 2: Good documentation practices in data integrity**

681  
682 Documentation should be managed with care. These should be appropriately designed in order to  
683 assist in eliminating erroneous entries, manipulation and human error.

### 684 685 *Formats*

686  
687 Design formats to enable personnel to record or enter the correct information at the right time.  
688 Provision should be made for entries such as, but not limited to, dates, time (start, finish, where  
689 appropriate), signatures, initials, results, batch numbers and equipment identification numbers. The  
690 system should prompt the personnel to make the entries at the appropriate step.

### 691 692 *Blank forms*

693  
694 The use of blank forms should not be encouraged. Where blank forms are used (e.g. to supplement  
695 worksheets, laboratory notebooks and master production and control records), the appropriate  
696 controls have to be in place and may include, for example, a numbered set of blank forms issued which  
697 are reconciled upon completion. Similarly, bound paginated notebooks, stamped or formally issued by  
698 a designated personnel, allow for the detection of unofficial notebooks and any gaps in notebook pages.  
699 Authorization may include two or three signatures with dates, for example, “prepared by” or “entered  
700 by”, “reviewed by” and “approved by”.

### 701 702 *Error in recording data*

703  
704 Care should be taken when entries of data and results (electronic and paper records) are made. Entries  
705 should be made in compliance with good documentation practices. Where incorrect information had  
706 been recorded, this may be corrected provided that the reason for the error is documented, the original  
707 entry remains readable and the correction is signed and dated.

## 708 709 **Example 3: Data entry**

710  
711 Data entry includes examples such as sample receiving registration, sample analysis result recording,  
712 logbook entries, registers, batch manufacturing record entries and information in case report forms.



713 The recording of source data on paper records should be in indelible ink and free from errors. Direct  
714 entry into electronic records should be done by responsible and appropriately trained individuals.  
715 Entries should be traceable to an individual (in electronic records, thus having an individual user  
716 access) and traceable to the date (and time, where relevant). Where appropriate, the entry should be  
717 verified by a second person or entered through technical means such as the scanning of bar-codes,  
718 where possible, for the intended use of these data. Additional controls may include the locking of  
719 critical data entries after the data are verified and a review of audit trails for critical data to detect if  
720 they have been altered. The manual entry of data into a computerized system should be traceable to  
721 the paper records used.

722

#### 723 **Example 4: Dataset**

724

725 All data should be included in the dataset unless there is a documented, justifiable, scientific  
726 explanation and procedure for the exclusion of any result or data. Whenever out of specification or  
727 out of trend or atypical results are obtained, they should be investigated in accordance with written  
728 procedures. This includes investigating and determining CAPA for invalid runs, failures, repeats and  
729 other atypical data. The review of original electronic data should include checks of all locations where  
730 data may have been stored, including locations where voided, deleted, invalid or rejected data may  
731 have been stored. Data and metadata should not be found in other electronic folders or in other  
732 operating system logs. Electronic data should be archived in accordance with a standard operating  
733 procedure. It is important to ensure that associated metadata are archived with the relevant data set  
734 or securely traceable to the data set through relevant documentation. It should be possible to  
735 successfully retrieve data and datasets from the archives. This includes metadata. This should be done  
736 in accordance with a procedure and verified at defined intervals.

737

#### 738 **Example 5: Legible and enduring**

739

740 Data and metadata should be readable during the life cycle of the data. Risks include the fading of  
741 microfilm records, the decreasing readability of the coatings of optical media such as compact disks  
742 (CDs) and digital versatile/video disks (DVDs), and the fact that these media may become brittle.  
743 Similarly, historical data stored on magnetic media will also become unreadable over time as a result  
744 of deterioration. Data and records should be stored in an appropriate manner, under the appropriate  
745 conditions.

## 746 **Example 6: Attributable**

747

748 Data should be attributable, thus being traceable to an individual. In paper records, this could be done  
749 through the use of initials, full handwritten signature or a controlled personal seal. In electronic  
750 records, this could be done through the use of unique user logons that link the user to actions that  
751 create, modify or delete data; or unique electronic signatures which can be either biometric or non-  
752 biometric. An audit trail that captures user identification (ID), date and time stamps and the electronic  
753 signature must be securely and permanently linked to the signed record.

754

## 755 **Example 7: Contemporaneous**

756

757 Personnel should record data and information at the time these are generated and acquired. For  
758 example, when a sample is weighed or prepared, the weight of the sample (date, time, name of the  
759 person, balance identification number) should be recorded at that time and not before or at a later  
760 stage. In the case of electronic data, these should be automatically date- and time-stamped. The use  
761 of hybrid systems is discouraged but where legacy systems are awaiting replacement, upgrade or  
762 connection to upper level systems, documented mitigating controls should be in place. (The  
763 replacement of hybrid systems should be a priority with a documented CAPA plan.) The use of a scribe  
764 to record an activity on behalf of another operator should be considered only on an exceptional basis  
765 and should only take place where, for example, the act of recording places the product or activity at  
766 risk, such as, documenting line interventions by aseptic area operators. It needs to be clearly  
767 documented when a scribe has been applied.

768

769 *“In these situations, the recording by the second person should be contemporaneous with the*  
770 *task being performed, and the records should identify both the person performing the task and*  
771 *the person completing the record. The person performing the task should countersign the*  
772 *record wherever possible, although it is accepted that this countersigning step will be*  
773 *retrospective. The process for supervisory (scribe) documentation completion should be*  
774 *described in an approved procedure that specifies the activities to which the process applies.”*

775 (Extract taken from the Medicines & Healthcare Products Regulatory Agency (MHRA) *GxP data*  
776 *integrity guidance and definitions (10).*)

777

778

779 **Example 8: Changes**

780

781 When changes are made to any result or data, the change should be traceable to the person who made  
782 the change and the date, time and reason for the change. In electronic systems, this traceability should  
783 be documented via computer generated audit trails or in other metadata fields or system features that  
784 meet these requirements. Where an existing computerized system lacks computer-generated audit  
785 trails, personnel may use alternative means such as procedurally controlled use of log-books, change  
786 control, record version control or other combinations of paper and electronic records to meet GxP  
787 regulatory expectations for traceability to document the what, who, when and why of an action.

788

789 **Example 9: Original**

790

791 Original data include the first or source capture of data or information and all subsequent data required  
792 to fully reconstruct the conduct of the GxP activity (*see the definition of raw data*). In some cases, the  
793 electronic data (electronic chromatogram acquired through high-performance liquid chromatography  
794 (HPLC)) may be the original data and, in other cases, the recording of the temperature on a log sheet  
795 in a room - by reading the value on a data logger – may be considered the original data. Original data  
796 should be reviewed according to the criticality and risk assessment. Proof of review should be  
797 presented (e.g. as a signature (reviewed by:) and date of the review). For electronic records, this is  
798 typically signified by electronically signing the electronic data set that has been reviewed and approved.  
799 Written procedures for data review should clarify the meaning of the review and approval signatures  
800 in order to ensure that the personnel concerned understand their responsibility as reviewers and  
801 approvers to assure the integrity, accuracy, consistency and compliance with established standards of  
802 the electronic data and metadata subject to review and approval. Written procedures for data review  
803 should define the frequency, roles and responsibilities and approach to review of meaningful metadata,  
804 such as audit trails. These procedures should also describe how aberrant data are to be handled if  
805 found during the review. Personnel who conduct such reviews should have adequate and appropriate  
806 training in the review process as well as in the software systems containing the data subject to review.

807

808

809

810

## 811 **Example 10: Controls**

812

813 Based on the outcome of the data integrity risk assessment (DIRA) (which should cover all areas of data  
814 governance and data management), the appropriate and effective controls should be identified and  
815 implemented in order to assure that all data, whether in paper records or electronic records, will meet  
816 ALCOA+ principles. Examples of controls may include, but are not limited to:

817

- 818 • the qualification, calibration and maintenance of equipment, such as balances and pH meters,  
819 that generate printouts;
- 820 • the validation of computerized systems that acquire, process, generate, maintain, distribute or  
821 archive electronic records;
- 822 • the validation of systems in order to ensure that the integrity of data will remain while  
823 transmitting between/among computerized systems;
- 824 • the validation of analytical procedures;
- 825 • the validation of production processes;
- 826 • a review of GxP records; and
- 827 • the investigation of deviations, out of trend and out of specifications results.

828

829 Points to consider for assuring accurate GxP records:

- 830 • the entry of critical data into a computer by an authorized person (e.g. entry of a master  
831 processing formula) requires an additional check on the accuracy of the data entered manually.  
832 This check may be done by independent verification and release for use by a second authorized  
833 person or by validated electronic means. For example, to detect and manage risks associated  
834 with critical data, procedures would require verification by a second person;
- 835 • formulae for calculations entered into spreadsheets;
- 836 • master data entered into the laboratory information management system (LIMS) such as fields  
837 for specification ranges used to flag out of specification values on the certificate of analysis;
- 838 • other critical master data, as appropriate. Once verified, these critical data fields should  
839 normally be locked in order to prevent further modification and only be modified through a  
840 formal change control process;
- 841 • the process of data transfer between systems should be validated;
- 842 • the migration of data including planned testing, control and validation; and

- 843 • when the activity is time-critical, printed records should display the date and time stamp.

844

845

\*\*\*

Draft for comments