16 December 2021

Submission of comments on *Guideline on computerised systems and electronic data in clinical trials (EMA/226170/2021)*

Comments from:

| Name of organisation or individual |
| --- |
| EFPIA |

*Please note that these comments and the identity of the sender will be published unless a specific justified objection is received.*

*When completed, this form should be sent to the European Medicines Agency electronically, in Word format (not PDF).*

1. General comments

| Stakeholder number  *(To be completed by the Agency)* | General comment (if any) | Outcome (if applicable)  *(To be completed by the Agency)* |
| --- | --- | --- |
|  | Overall, the draft guidance is very robust, comprehensive, and provides all stakeholders with the Agency’s expectations on use of computerised systems in clinical research and on the collection of variety of electronic data. The draft guidance document is a very useful resource about the level of transparency EMA seeks from stakeholders on this topic. We look forward to future Annex around the use of Artificial Intelligence in clinical trials. |  |
|  | The topics and content make sense; however, the document is rather long, too detailed and there is repetition/duplication of concepts.  The Guideline is quite descriptive in multiple cases providing the solution vs. expectations posing constraints.  The Guideline has duplicative content or industry defined content relating to electronic data, data, computerized system, computerized system validation, and security. We suggest simplifying this document to consolidate key aspects/requirements of the Authority, provide reference to Industry standards such as data integrity, ALCOA++, etc.  From a general perspective we see a need to simplify and streamline this document prior to releasing it for public use. |  |
|  | The scope is extremely wide. In today’s world, we question the feasibility of an individual sponsor qualifying and getting access to validation documentation for all these systems, apps, software etc. It will be a challenge to know about all of these and do a risk assessment of all subcontracted systems. It may be more practical if certain standard providers like SAS, MediData, Veeva Vault, Apple Health app, etc. would be certified to provide these services to GCP compliant clinical trials.  There is a grey area as to system versus trial specific guidance. Some sections refer to system, others to the trial protocol.  As a general guidance it would be beneficial to differentiate clearly between these topics.  We would suggest clarifying the context of the document as it relates to the use of computers systems within clinical trials versus how to validate a computer system.  We would suggest to cover guideline for the need of validation/qualification of software/tools used as part of the development of the computerized system. |  |
|  | As stated by the Agency in the strategic reflection titled “EMA Regulatory Science to 2025”, there is an urgent need to develop the regulatory framework for modernization of GCP oversight to enable emerging clinical data generation and decentralized models of clinical trials, coupled with direct digital data accrual.  To leverage new technologies and innovation for accelerating progress in clinical research, international collaboration across regulatory agencies is critical for uniform directions, which based on risks, can illuminate the most modern challenge areas.  As a sponsor, we should ensure that all aspects of the clinical trial are operationally feasible and avoid unnecessary complexity, procedures, and data collection (ref. ICH GCP 5.0).  Our commitment to fulfill this foundational GCP requirement is sustainable if regulatory guidelines are homogenous, realistic, based on risks, and achievable to all stakeholders.  After careful reading of the draft guidance, we recommend the Agency to:   1. **Enable modernization by**   - outlining their position on emerging technologies for direct digital data capture beyond eCOA solutions (e.g., telemedicine, digital health technology (DHT), apps, wearables, robots and artificial intelligence, etc.) as per their strategic reflection paper (e.g., section 6). For eCOAs, the guidance focuses on ePROs and ClinROs; however, there are other categories of eCOAs that can be collected via computerised systems, such as PerfOs and ObsRos. We kindly suggest to the authors to consider adding more guidance for PerfOs collected via sensors / wearables as their use will increase considerably in the near future.  - reconsidering certain expectations that appear discouraging and biased towards paper formats as the preferred standard, to support innovation in clinical investigations and healthcare systems; this guidance is biased towards traditional paper-based systems specifically in the realms of informed consent; with the increasing digital age, it would be helpful to have a better balance between paper and digital (eg., lines 408, 708, 610-611, 635-636 1588-1589);  **B) Define realistic and achievable expectations by**  - revising burdensome requirements that are not providing additional assurance of data quality or benefit to participant safety. For instance:   * Description of detailed operational activities in the protocol, leading to unnecessary deviations (e.g., lines 464-469, 484-485, 1347-1348, 1382-1383, 1591-1592). It is mentioned in different places in the draft guideline that things need to be stated – we would advise against having this mean that everything should be stated in the protocol, but rather in documents referred to in the protocol; we would like to avoid a situation where we would face multiple protocol amendments because of operational information which may change more often.   + Increased frequency of investigator signature, regardless of the type of data collection tools (eCRF vs. ePRO), type of data originators (person vs. device), monitoring and despite site-owned policies for delegation and oversight (e.g., from line 706 to 739).   + Collection of investigators’ signatures on eCRF data prior to data release to external committees for independent reviews, potentially introducing bias, despite the limited contribution of eCRF data to those conclusions (lines 721, 722)   + Centralization of all the different events from a given process into one burdensome deliverable, requiring maintenance and retention (e.g., from line 479 to 482)   + Validation of each data transfer, disregarding use of validated processes that provide assurance of data integrity (e.g., lines 613-614, 619-621)   + Capture the edit check as part of the change rationale in the audit trail, impacting the collection of the true reason for changes or create conflicts when an edit check fires but the data changes are in a different data source - e.g., reconciliation check between forms or databases (ref. to lines 682-684) * Restoration of decommissioned electronic data capture systems (e.g., eCRF, eCOA, ePRO), without considering the high risks to invalidate the archived certified copies by continuous transition or migration of data/metadata to enable restoration of obsolete/unlicensed technologies (ref. to line from 883 to 888) * Ability to archive in a dynamic format for long time periods considering technology and infrastructure advances are technically challenging. We recommend the use of a "fit for purpose" construct instead of articulating a dynamic format requirement. (Refer to lines 385 and 888)   **C) aligning with other regulatory agencies.**  For instance:   * on a practical position for collection of investigators’ evidence of supervision on reported data to sponsor. In light of new technologies, existing controls to mitigate data integrity risks (at sponsor and at site), we recommend the frequency being governed by data submission timepoints to Agency(ies) and prior to archival. (see details in Section 2 of this document, comments to lines 706-739); * Please consider harmonization in the use of electronic informed consent platforms and e-signatures amongst local health authorities. |  |
|  | The document notes specific areas where shortcomings would be considered GCP non-compliance. The text tends to be quite prescriptive and some older systems may not be able to be brought to current standard, yet users may have identified alternative means to document / justify. Some consideration should be provided in the text that allows for continued use of legacy systems. |  |
|  | The overall scope of the technology covered is broader than Electronic Data Capture (EDC), however, examples are typically limited to EDC. Consideration to referencing types of system should be clarified, especially as the investigator should have access to all data collected by site / patient during the clinical trial - at least a reference to Annex 5 for additional system when noting EDC should be included as an example in other sections. |  |
|  | Risk-based approach and criticality of data requires further explanation and guidance. The document should include some relevant examples of assessment and how to document. |  |
|  | Please consider adding more text around data collection via the Internet of Medical Things (IoMTs) which is a means of integrating medical devices, sensors and wearables with healthcare information technology systems by using networking technologies. This is explained in a recent position paper by the European CRO Federation and the eClinical Form; Version A 2021-02-24. The title of the paper is “Trial Master File Archiving and the Decommissioning of Computerized Systems used in Clinical Trials.” Section 5.1 of the above-mentioned paper suggests that “Devices that continuously collect data (wearables, patches, sensors, etc.), sometimes characterised as IoMT (Internet of Medical Things) devices, can collect huge amounts of raw data that are pre-processed within the device or vendor portal. These are called aggregate data collectors, and they result in only cumulative or aggregate values being uploaded and retained – the raw data is used to generate the aggregate data. The clinically meaningful measurement values, which are the aggregated results of the data collected, must be defined within the protocol so it is clearly understood what data are being uploaded, saved and archived. It is these aggregated values that are the source data.” |  |
|  | There is no section in the guideline about emergency changes, i.e., changes required to solve a critical or security issue which should be deployed as fast as possible (before formal testing and documentation activities). |  |
|  | We would suggest to cover guideline in regards to CSV records and the controls expected for the creation, review, approval and maintenance: e.g., following good documentation practice. |  |
|  | Separate sign off for single CRF pages/batches is difficult to establish with current CRF provider(s). Therefore, an overall revision/new considerations regarding timing and frequency vs. purpose for sign off guidance may be valuable. |  |
|  | It is recommended that guidance be provided regarding data integrity/interpretation of data where studies will be using hybrid models (e.g., where some patient’s assessments are conducted at sites and others are conducted remotely through wearables), the risk management requirements and related monitoring requirements. |  |
|  | Considerations should be given to other documents (i.e., GAMP 5, ICH E6) that already outline/define computer systems validation, ALCOA+ etc. We would suggest that terms that have been defined in other documents are not duplicated in this glossary. |  |
|  | Throughout the document reference is made to “responsible party/ies”. Clarification is requested as to how this party is defined in the various references. |  |
|  | The document references “tools”, “computerised systems”, “devices”, and “applications”, sometimes interchangeably. Could you please define each or clarify? |  |
|  | We would suggest adding the definition of the terms “Approval” and “Authorized in writing” in the “Glossary and abbreviations” section. |  |
|  | The document is overly expressive and contains numerous subjective words or statements that leave the guidance open to interpretation. We would suggest removing subjective statements or defining descriptive terms such as “critical”, “important”, “should” vs “shall”, “acceptable”, “should be clear”, “adequate”, “significant”, “insignificant”. |  |
|  | We would suggest reviewing the document for grammar. Also, in many places in the document “or” is used when it should be "and/or". |  |
|  | We suggest to use the term “records” rather than “document”, where the latter is not explicitly expected to be stored as information in a document-like format (e.g. pdf). Example in line 1036: *“The sponsor/investigator should take responsibility for the URS. This document should always be reviewed and approved by the sponsor/investigator.”*  Whatever terminology is used (data, document, documentation, record, etc.), it should be clear that this does not bind industry to a specific format (as long as the format is ‘fit for the intended purpose’, including that it is human readable).  Some documentation for a computerised system and its qualified/validated state are more and more often stored in a “distributed” manner, for instance in a tool supporting the agile methodology (e.g., Azure DevOps or Jira), where the user requirements are not stored as a document, but as e.g., a number of epics or user stories, and where a document (report) containing the consolidated set of current user requirements may be produced at request. |  |

1. Specific comments on text

| Line number(s) of the relevant text  *(e.g. Lines 20-23)* | Stakeholder number  *(To be completed by the Agency)* | Comment and rationale; proposed changes  *(If changes to the wording are suggested, they should be highlighted using 'track changes')* | Outcome  *(To be completed by the Agency)* |
| --- | --- | --- | --- |
| 122-140 |  | **Comment:** Please add definitions in the section “Glossary and abbreviations” for the following:   1. closed and open systems which are discussed in section “4.8 Electronic Signatures” (line 491) 2. decentralized and partially decentralized trials which are discussed in the Executive Summary (line 243) 3. “fallback procedure” – apparently a technical term, not commonly used - either provide a definition or add details in the related section of the guidance (line 1427) 4. “Traditional V-Model” or “agile principles” since the audience may not be familiar with such terminologies (line 1024) 5. Metadata 6. ***Critical*** and ***Non-Critical*** data   **Proposed change (if any):**  For *closed and open systems,* we propose aligning with the FDA definition from 21 CFR Part 11.  We propose the following definition for decentralized and partially decentralized trials:  “Decentralized clinical trials (DCT) are trials that bring the trial execution closer to the patient by enabling study procedures away from the investigator site to locations more convenient for study participants, including at home, telehealth, mobile visits, and community-based healthcare setting such as local HCPs/imaging centers/laboratories. Data are captured remotely using mobile technologies in these more participant convenient locations. DCTs can include fully decentralized approaches and varying levels of decentralization also known as partially decentralized or hybrid approaches.” |  |
| 127-128 |  | **Comment:** The reference to CRO being equated with Sponsor is unclear. CRO seems to equal Sponsor, but Sponsor does not equate to CRO with regards to data visibility/access.  Please clarify the distinction, based on responsibilities and access to a computerised system, between CRO and Sponsor. The software vendor should be included separately as well. |  |
| 134 |  | **Comment:** The “subject” definition should be extracted from Regulation 536/2014 (Clinical Trials Regulation - CTR) instead of Directive 2001/20/EC, as the CTR will be in place when the guidance is in place. The definition for ‘subject’ is similar in both legislations.  **Proposed change (if any):**  “The word "trial participant" is used in this text as a synonym for the term “subject”, defined in Regulation 536/2014 ~~Directive 2001/20/EC~~ as “an individual who participates in a clinical trial as a recipient of the investigational medicinal product (IMP) or a control.” |  |
| 137 |  | **Comment:** "data" has already been defined in lines 125-126. Please remove duplication of definition of “data”.  **Proposed change (if any):**  “For the purpose of this guideline, the term “information” reflects meaningful organisation and processing of data and documentation ~~and “data” reflects measurement and assessment of variable parameters relevant to specific outcomes~~.” |  |
| 139, 540 & 1562 |  | **Comment:** The term “fit-for-purpose” is used without providing a definition in the Glossary section.  **Proposed change (if any):**  **Addition**  Please provide a definition of the term “fit-for purpose” in the Glossary section, ideally in alignment with US FDA recommendations for drug development tools. |  |
| 141 |  | **Comment:** AI is a broad general field of study, and it includes ML, but ML is not the only sub-category of AI, just like saying a wheel (ML) is the same thing as a car (AI). Also consider computer vision, robotics, natural language processing, fuzzy logic, etc. Several schools of thought on the categories:  https://www.freecodecamp.org/news/ai-vs-ml-whats-the-difference/ and https://serokell.io/blog/ai-ml-dl-difference and https://www.bmc.com/blogs/artificial-intelligence-vs-machine-learning/ and https://www.edureka.co/blog/types-of-artificial-intelligence/ are some examples. |  |
| 144-146 |  | **Comment:** The model may somewhat incorporate repetitive recalibration / re-calculations to "refit" the models over time.  Is the terminology of “supervised” and “unsupervised” widely understood or would examples be needed here? Also consider “semi-supervised” and “reinforcement learning” - reinforcement learning is also a type of Machine Learning.  https://flatironschool.com/blog/deep-learning-vs-machine-learning  **Proposed change (if any):**  “Machine learning (ML) is a subset of AI and includes computer algorithms which are trained to classify or predict data, without ~~actually~~ being explicitly programmed to do so. ML is divided into supervised ~~and~~ unsupervised, semi-supervised and reinforcementlearning.” |  |
| 147-148 |  | **Comment:** This "exposing multi-layered neural networks" may be only one type of Deep Learning. It is overly descriptive and may soon, if not already, be out of date. Even simple ML models can be programmed to self-train (recalibrate) if programmed properly.  Please consider the difference between DL and reinforcement learning. One layman’s reference is: https://www.forbes.com/sites/bernardmarr/2018/10/22/artificial-intelligence-whats-the-difference-between-deep-learning-and-reinforcement-learning/?sh=57e448e8271e  **Proposed change (if any)**:  “Deep learning (DL) is a subset of ML and contains algorithms which allow software to train itself by exposing ~~multi-layered neural networks~~ to vast amounts of data.” |  |
| 149, 151-153 |  | **Comment:** We would suggest deleting the term "access" from the definition.  Access to the system should be audit trailed (e.g., via an access log) but few systems audit trail access to individual records (e.g., read only access) as the expectation of audit trails for records has been to record creation, modification, and deletion but not access. An event log is a good descriptor for the "use of the computer system" which may have different regulatory applicability.  **Proposed change (if any)**:  “In computerised systems an audit trail is a secure, computer-generated, time-stamped electronic record that allows reconstruction of the ~~course of~~ events relating to the ~~access,~~ creation, modification, ~~and~~ or deletion of an electronic record ~~or use of the computerised system itself~~.”  **Addition**  Please consider adding a new entry for “Event Log” that records user activity in relation to use of a system that may not affect data. |  |
| 161-165  &  194-200 |  | **Comment:** The COA definition in the glossary could be more accurate (currently missing PerfOs) and propose to include PRO in COA definition as opposed to having a separate definition.  **Proposed change (if any**):  Proposed wording of Clinical outcome assessment (COA) definition in the glossary, which replaces the current draft and is combined with the definition of PRO:  “A COA is a measure that describes or reflects how a patient feels, functions, or survives. There are four main types: clinician-rated outcome assessment (ClinRO), Observer-reported outcome assessment (ObsRO), Patient-reported outcome assessment (PRO) and performance outcome assessment (PerfO). The term COA is proposed as an umbrella term to cover both single dimension and multi-dimension measures of symptoms and impacts of disease.”  A PRO can also be designed to facilitate communication with patients in order for investigators to assess and evaluate patient-reported adverse events and medical history, which will not be directly collected using ePRO as outcome measurements.” |  |
| 163-164 |  | **Comment:** Consider the difference between signs (observable and objective – e.g., a skin rash) versus symptoms (subjective – e.g., nausea). |  |
| 173 |  | **Comment:** The scope and definition of “dynamic data files” could be clearer. Different descriptions and examples are used in the different data integrity guidelines. Some more alignment across the guidelines would be preferable.  The use of “dynamic file” in other places of the document confuses this definition. For example, in the section on audit trails (line 657) it is stated that audit trails should be “available as an exported dynamic data file”; but the definition of this type of file indicates its content can be changed; which is inconsistent with what audit trail data should be.  If this applies to any dynamic file format, does this statement imply that changes should be audit-trailed? If so, it might make sense to specifically say so since multiple versions may exist during the life cycle of the document.  In addition, it is suggested to consider the combination of file formats and tool capabilities, as it is this combination that determines the ability to interact in a dynamic way with the data.  **Proposed change (if any):**  “Dynamic files (e.g. spreadsheets with automatic calculations) include automatic processing, data restructuring and analysis (e.g., filtering, transposing) and/or enable an interactive relationship with the user to change content (e.g. eCRF).” |  |
| 174-176 |  | **Comment:** We suggest clarifying the retention duration of the dynamic file formats in the guidance document. To retain the dynamic file formats of any electronic utility/tools or applications for extended duration will be burdensome to stakeholders and will likely increase the overall cost of clinical trials. We would suggest a similar approach than to the ICH GCP requirement retention of clinical research documents: ‘until at least 2 years after the last approval of a marketing application in an ICH region and until there are no pending or contemplated marketing application in an ICH region or at least 2 years have elapsed since the formal discontinuation of clinical development of investigation product.” We suggest stating in the guidance that sponsors and other stakeholders should retain dynamic file formats for at least 2 years after the last approval of a marketing application in an ICH region.  After this period, the equivalent static file formats including metadata should be available for any inspection or legal requests.  **Proposed change (if any):**  “A certified electronic copy may be retained in different electronic file formats to the original record, but the equivalent dynamic nature (including metadata) of the original record should be retained at least 2 years after the last approval of a marketing application in an ICH region.” |  |
| 177 |  | **Comment:** Please consider adding a section or subsection under 4.5 ALCOA+ for “Good documentation practice” and shorten the definition. Consider using in the glossary the existing definition:  **Proposed change (if any):**  **Addition**  Please add a subsection under 4.5 ALCOA+ for “Good documentation practice” before line 388 and provide the following description of it:  “Good documentation practices are those measures that collectively and individually ensure documentation, whether paper or electronic, is secure, attributable, legible, traceable, permanent, contemporaneously recorded, original and accurate.” (ref. WHO Annex 5) |  |
| 181 |  | **Comment:** “in notebooks” is too broad an example.  **Proposed change (if any):**  “that critical entries are verified by a second person, that pages (e.g. in laboratory notebooks) are numbered” |  |
| 183 |  | **Comment:** Consider revising the sentence in a sense that GXP changes could also state the initials instead of the name.  **Proposed change (if any):**  “The latter implies that changes include the name or initials (if name and initials are kept elsewhere) and the signature of person who made the change” |  |
| 185-186 |  | **Comment:** Is it needed to explain the term “relevant” (in which context)? (versus line 400: “Accurate date and time information should be automatically captured…”)  **Proposed change (if any):**  “the date and only if relevant the time when the change was made” |  |
| 188-189 |  | **Comment:** The guideline **s**hould include a reference to data integrity principles so people can maintain the link between ALCOA++ and them.  **Proposed change (if any):**  There is a strong bond between good documentation practice and the ALCOA++ principles (see sections 4.1 and 4.5 ~~4.4~~) and between GxP corrections and an audit trail (see section 6.2).” |  |
| 191 |  | **Comment:** A Definition of ‘critical documents’ is missing.  **Proposed change (if any):**  **Addition**  Please provide a definition of the term “critical documents” in the Glossary section, where necessary. |  |
| 192 |  | **Comment:** It is suggested to only use “signed when subject to a predicate rule”. Other approval mechanisms may provide adequate proof of who approved. This should be verified with the EU GMP reference to see if they state what exactly “essential documents” (or records) are that require a signature or initials.  **Proposed change (if any):**  “~~In general,~~ essential documents should be approved, signed (as and where required by applicable laws and/or guidance documents) and dated by the relevant/authorised persons. See also EU GMP Chapter 4. |  |
| 195 |  | **Comment:** An outcome may also be reported by participant parent(s), guardian(s) or caregivers.  **Proposed change (if any):**  “Any outcome reported directly by the trial participant, participant parent(s), guardian(s) or caregivers and based on…” |  |
| 199 |  | **Comment:** The use of HRQL measures should be described in more details in the Patient Related Outcome (PRO) section. |  |
| 208 |  | **Comment:** We noted the use of “Source” as opposed to “Raw” data. For certain laboratory analyses this can be an important distinction. For example, a chromatographic analysis may have the “raw” data being the actual digital datapoints collected while the analysis is running. The integrated results as first reported also becomes a type of “Source” data or record, but is not the “Raw” data.  **Proposed change (if any):**  **Addition**  Please provide a definition of Raw and Source data, clarifying differences between the two. |  |
| 220-222 |  | **Comment:** We would suggest removing the example of PDF scan because PDFs have become much more advanced (i.e., in the future, changes could be made that are not obvious.)  Some file formats (e.g., text files) are neither “Dynamic file formats” nor “Static file formats”. It is suggested that a definition for other types of formats be included.  **Proposed change (if any):**  “Static files ~~(e.g. PDF scan)~~ containing information or data that are fixed~~/frozen~~ and allow no interaction to change the content, e.g., a paper document digitised as pdf~~, e.g.~~ such as scanned ethics committee approval letter.” |  |
| 224 |  | **Comment:**  The regulated party may also support the process.  **Proposed change (if any):**  “i.e. typically 1) the concept phase where the regulated party considers supporting and/or automating ~~to automate~~ a process and where user requirements are collected” |  |
| 225 |  | **Comment:** We would recommend the inclusion of hybrid systems in the scope. Additionally, the definition for a hybrid system should be included, which is a system that includes combinations of paper records (or other non-electronic media) and electronic records, paper records and electronic signatures, or handwritten signatures executed to electronic records. |  |
| 226 |  | **Comment:** The selection of a third party is optional.  **Proposed change (if any):**  “2) the project phase where a contracted party can be ~~is~~ selected, a risk-assessment is made and the system is implemented and ~~qualified~~ validated” |  |
| 228-229 |  | **Comment**: ‘*maintains data confidentiality, integrity and availability’*:  Does it need to be explicitly stated that the changes to the system do not have deleterious effects on functionality in addition to everything else listed here? What about “bug fixes”? Is all of that implicit or does it need to be defined? |  |
| 237 |  | **Comment:** Please consider the following corrections and additions under “Abbreviations”.  **Proposed change (if any)**:  - “commercial off ~~of~~ the shelf” (on line 977 as well)  - “electronic data ~~collection~~ capture”  - “International ~~Conference~~ Council ~~on~~ for Harmonization”  - “international mobile e~~E~~quipment identity”  - “mobile equipment~~\_~~identifier” (There is an underscore between equipment and identifier)  **Additions**   * ECG/EKG for electrocardiogram * eIDAS for electronic identification and trust services * IVRS/IWRS for interactive voice response system/interactive web response system * (e)PRO for electronic Patient-Reported Outcome * Other cloud computing types than IaaS, SasS, PaaS and FaaS and public/private/hybrid clouds should probably be provided.   For example: https://www.vxchnge.com/blog/different-types-of-cloud-computing |  |
| 255 |  | **Comment:** It is not clear if the scope intends to cover Electronic Health Record (EHR) systems for clinical trial data collection purposes. Specifically, when an EHR system has expanded capability to enable clinical trial data collection (either direct data capture or transcribe from health records), then data is transferred to the EDC system electronically instead of manually entered into the EDC.  Please clarify.  We recommend including acceptable mitigations for the use of Electronic Health Records. The guidance lacks expectations on evaluation, mitigation, and monitoring of these systems as was included in the reflection paper titled “Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials”, section 6.3. |  |
| 256 |  | **Comment:** We would suggest to include a section under “scope” that explicitly summarizes the types of data in scope of the guidance (rather than just implying the types of data in scope based on computerised system examples).  It is not clear whether the guidance includes or excludes clinical trials with devices.  **Proposed change (if any):**  **Addition**  Please add a section under “scope” that explicitly summarizes the types of data in scope of the guidance. |  |
| 256-293 |  | **Comment:** We suggest including Direct Data Capture (DDC) mentioned in section 6.1.3 (line 627) in this scope section as well. Although lines 262-266 mention a few Direct Data Capture data sources, we suggest to include DDC for better clarity. |  |
| 260, 267, 274-277 |  | **Comment:** For electronic Health Records and for tools used such as blood pressure monitoring, ECG monitoring, Xray machines, etc.:  What needs to be checked by the sponsor at the site - is it validation process/ documents? Will each of the hospital’s commonly owned e-system/ instrument’s validation status/ process/ documents need to be checked for the clinical trial?  The terms “in a clinical environment” and “in support of clinical trials” are used here. For clarification: if, for example, the clinical site is a hospital, and the hospital x-ray machines and blood sample analysis laboratories are used to generate source data for the clinical trial, are the x-ray machine and the laboratory systems in scope of this guideline?  Note: If such systems need to be assessed and/or validated by the sponsor, then this is a significant additional burden to conduct clinical trials. It is also potentially straining the relationship between sponsors and principal investigators considerably. Also, current CRAs are typically not trained for assessing computerized systems. This will therefore require the introduction of a new type of specialist among the CRAs. |  |
| 262-267 |  | **Comment:** We would suggest to refer to eCOA data rather than making specific references to ePRO and clinician rated COAs captured electronically.  Clarification is required as to whether this refers only to tools supplied by the sponsor.  For ‘*mobile devices supplied to clinicians’*, does this apply only to clinical trials or would it apply in post-market studies and general practice outside of clinical studies as well?  **Proposed change (if any):**  “Digital Health Tools supplied to investigators, ~~/~~trial participants and/or study partners for electronic recording of clinical outcome assessments ~~data by data entry~~ (~~e.g.~~ COAs), including:   * Electronic trial participant data capture devices used to collect ePRO data, e.g. mobile devices supplied to trial participants or applications for the use by the trial participant on their own device (bring your own device (BYOD)). * Electronic devices used by clinicians to collect data e.g. mobile devices supplied to clinicians. * Tools supplied for automatic capture of events such as biometric measures, wearables, sensors and image capture devices that capture data from trial participants” |  |
| 272 |  | **Comment:** Does the term "tools" include probes that monitor temperature or does it refer only to the software which manages the data collected by the probes? Does computer systems validation encompass instrument calibration? |  |
| 289-290 |  | **Comment:** Some software types are duplicated.  Systems used to upload information to event adjudication committees should also be covered by the list.  **Proposed change (if any):**  “Other computerised systems implemented by the sponsor holding/ managing and/or analysing data relevant to the clinical trial e.g. clinical trial management systems (CTMS), pharmacovigilance databases, statistical software programming ~~pharmacovigilance databases~~, statistical software, document management systems and central monitoring software.” |  |
| 293 |  | **Comment:** Systems/tools used by Sites or Sponsors to conduct remote activities such as remote monitoring, remote source data verification or remote auditing and tools related to Telemedicine to conduct remote visits should be incorporated in the scope.  **Proposed change:**  **Additions**  “Systems/tools used by sites or sponsors to conduct remote activities such as remote monitoring, remote source data verification or remote auditing and tools related to telemedicine to conduct remote visits” |  |
| 294 |  | **Comment:** “*The approach towards computerised systems and medical devices used in clinical practice”* – we would suggest clarifying “*medical devices”* in the text as it could be confusing as medical devices are also subject to other regulations (Medical Device Regulations) unlike the computerized system validation.  To avoid any ambiguity, we would suggest adding a statement that clarifies which aspects related to the use of medical devices in a clinical trial are not the subject of this guideline and are regulated under the Medical Devices Regulation.  **Proposed change (if any):**  “The approach towards computerised systems (incl. ~~and~~ medical devices used in clinical practice if they are used within the clinical trial to collect any clinical trial data) ~~(e.g. regarding validation)~~ should be risk proportionateand any other applicable regulations (e.g. Medical Device Regulation) should be applied.” |  |
| 299-302 |  | **Comment:** In general, we appreciate this section which allows a risk-based approach to systems used in clinical practice.  This section talks about two scenarios:  - Computerized Systems with less critical data for which the proposal of a certification by a notified body should be clarified;  - More critical systems for which in-depth validation effort for critical systems is clear.  It is not clear what would be ‘less critical data’ for which systems.  Assuming the justification would be made to the appropriate regulatory agency such as EMA, should that be stated here?  Clarification is requested for the scenario where additional validation efforts would be required and how critical vs. non-critical systems are defined.  Systems used for Critical data critical systems v/c noncritical systems: This decision should be justified pre-trial. Can the sponsor’s decision be challenged later by inspectors? Is the investigator expected to be the decision-maker for the site systems?  “Approved Setting” is not clear in the statement. What is meant by approved setting?  It is proposed to define clearly what is meant by approved setting.  “Well established” is not clear. The word “Legacy” should be used instead.  In case of well-established computerised systems, which are used in line with approval in a routine setting for less critical trial data, the certification by a notified body may suffice as documentation whereas other more critical systems may require a more in-depth validation effort. This decision should be justified pre-trial.  If a well-established system, which has been approved for use in patient care, is used to generate source data from which primary efficacy data is derived, would that system need to be validated?  It is not clear where a notified body would fit with the assessment of anything other than medical devices.  **Proposed change (if any):**  Line 299: “Systems used outside the approved setting are ~~is~~ inherently of higher risk. In case of ~~well-established~~ legacy computerised systems,…”  Line 302: “This decision should be justified and documented pre-trial.” |  |
| 301 |  | **Comment:** Certification by a third party cannot be a substitute for the regulated company performing validation (as implied by this text), no matter how well established a CS may be. Certification may support some risk-based decisions (e.g., to reduce the level of security testing if a service is ISO27001 certified).  **Proposed change (if any):**  Please change the content to be clear on how third-party certification can be used. |  |
| 308 |  | **Comment:** Is GDPR included here? |  |
| 312-314 |  | **Comment:** The guidance describes areas where institution / investigator are involved / responsible (e.g., source documentation). This should be clearly stated.  **Proposed change (if any):**  “The guideline applies to the legal representatives, ~~and~~ CROs and institutions / investigators, which …” |  |
| 314-342  468-469  484-485 |  | **Comment:** The term ‘GCP non-compliance’ is too strong to be used in a guidance.  **Proposed change (if any):**  Line 342: “equivalent to data loss/destruction ~~and is considered GCP noncompliant~~.”  Line 469: “to be source data ~~is considered as GCP-noncompliant~~.”  Line 485: “that is not stated in the protocol or related documents ~~is considered GCP-noncompliant~~.” |  |
| 315-316 |  | **Comment:** The risk-based approach, besides use of computerized systems and collection of electronic data, also has an impact on monitoring of electronic data.  **Proposed change (if any):**  “The risk-based approach to quality management ~~also~~ has an impact on the use of computerised systems and collection (as well as monitoring) of electronic data.” |  |
| 317 |  | **Comment:** *“comes into application”* does not sound correct.  **Proposed change (if any):**  “the Clinical Trials Regulation (EU) 317 No. 536/2014 (‘Regulation’) ~~comes into application~~ becomes applicable” |  |
| 321 |  | **Comment:** We would propose to delete "e.g." if devices are to be included.  Meeting frameworks for electronic identification also needs to be considered. It is unclear whether this is intended to be captured under “electronic identification” but, in any case, this should be referred to specifically.  **Proposed change (if any):**  “These may include ~~e.g.~~ , but are not limited to, medical devices, data protection legislation and legislation on electronic identification and electronic signature.” |  |
| 329-332 |  | **Comment:** We would suggest defining what is “a secure manner”. The text should also refer to Annex 4, Security.  The different concepts of ALCOA vs. ALCOA+ vs. ALCOA++ need explanation either under 4.5 or in the Glossary. 4.5 only defines the aspects without differentiation. Alternatively, a reference to a source could be included (also relating to 4.5 and Glossary).  “Available” is listed as ALCOA ++ definition in Section 4.5. However, "available" is omitted from Section 4.1.  **Proposed change (if any):**  “For this section reference is also made to Annex 4, Security.Data integrity is achieved when data (irrespective of media) are collected, accessed and maintained in a secure manner, to fulfil the ALCOA++ principles of being attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, available when needed and traceable as described in section 4.5” |  |
| 335 |  | **Comment**: “*Data governance”* is another good aspect to consider in evolving cloud-based environments. |  |
| 340 |  | **Comment:** It is suggested replacing *“undesirable results”* with *“unexpected results”* based on system issues as this more accurately reflects the nature of these results.  **Proposed change (if any):**  “…and actively encourages reporting of errors, omissions, and ~~undesirable~~ unexpected results.” |  |
| 341 |  | **Comment:** We would propose the following change, for clarity.  **Proposed change (if any):**  “Lack of integrity before the expiration ofthe mandated retention period can ultimately render the data unusable” |  |
| 342 |  | **Comment:** one can have compliant data destruction practices - especially at the end of the data retention lifecycle. It would be preferrable to just keep it as equivalent to data loss.  **Proposed change (if any):**  “and is equivalent to unintended data loss/destruction” |  |
| 344 |  | **Comment:** We would like to propose the following change for clarity.  **Proposed change (if any):**  “Roles and responsibilities in clinical trials should be ~~clear~~ clearly defined.” |  |
| 344-346 |  | **Comment:** The *“clinical trials context”* at the end of the sentence is redundant because this is already established at the beginning of this sentence.  **Proposed change (if any):**  “The responsibility for the conduct of clinical trials is assigned via legislation to two parties, which may each have implemented computerised systems for holding/managing data~~, in the context of clinical trials~~” |  |
| 347-349 |  | **Comment:** Clarification is requested regarding whether the expectation that investigators and institutions are also to validate their systems to the same standards as sponsors and whether regulators will evaluate the validation of systems owned/managed by investigators and institutions that are not provided or supported by sponsors. |  |
| 347 & 350 |  | **Comments:** Reference to *“storing the data”* would also be advisable.  This section should include reference to software vendors and software-as-a-service vendors.  **Proposed change (if any):**  Line 347: “Investigators and their institutions, laboratories and other technical departments or clinics, generate and store the data, etc.”  Line 350: “Sponsors, supplying, storing and/or, managing and operating computerised systems (including software and instruments) and the records generated by them.” |  |
| 352 |  | **Comment:** IWRS should also be included in this section as well as in the abbreviations (see line 237).  We are also unsure why the term “specialists” is in this section.  **Proposed change (if any):**  “or interactive voice**/**web response system (IVRS**/**IWRS) specialists that collect and store data on behalf of sponsors.” |  |
| 354 |  | **Comment:**  Tasks related to computerized systems might cover development, implementation, deployment and use of systems, but also use of systems as part of service provision by third parties.  **Proposed change (if any):**  “Please refer to Annex 1 regarding the contracting out of tasks related to the use of computerised systems and services.” |  |
| 355 |  | **Comment:** The section name is *“Electronic data”*, however the details in the section are primarily talking about what is a data and metadata. The data which is considered Electronic data is not clearly defined.  Section 4.3 offers the definition of Data and metadata, both could be moved to the glossary. If left in this section, there should be a need defined, e.g., each data point should have its relevant metadata values that allow to verify its integrity.  **Proposed change (if any):**  **“**Electronic data and Metadata” |  |
| 356 |  | **Comment:** *“collected”* is not needed in this sentence.  **Proposed change (if any):**  “Electronic data consists of ~~collected~~ individual data points.” |  |
| 362 |  | **Comment:** It should be stressed that the loss or corruption of metadata (e.g., audit trail) before the mandated retention period can also lead to lack of integrity and can ultimately render the data unusable and is equivalent to data loss/destruction and is considered GCP noncompliant. |  |
| 363-386 |  | **Comment:** We suggest that the Agency clarifies in Section 4.4 what *“source data”* would be for a wearable device. For example, in the case of an accelerometer with a 32 Hz sampling rate, would epoch (e.g. minute-by-minute) level data from which the clinical trial endpoints (e.g. activity counts/day) can be calculated be sufficient as the *“source data”*? Or would the raw 32 Hz x,y,z data need to be retained and transferred to the sponsor as the *“source data”*? |  |
| 364-365 |  | **Comment:** *“However, source data can be processed to a certain degree.”* A more specific wording would be beneficial. |  |
| 364-383; Section 4.6, 4.10 |  | **Comment:** The scope of computerized systems/electronic source responsibility should be made clearer in the guidance in these circumstances. The responsibility for validation is well described as belonging to the system owner in section 4.10, but less well in section 4.2. The validation of site related systems used in standard of care practice for all site patients (CT/MRI scan, electronic medical record), including clinical trial participants, should be the responsibility of the site.  The sponsor requirements for site systems would be limited to asking basic question(s) as to whether the site has done due diligence and could respond to an inspector/auditor questions regarding their systems validation – see section 5.0.  Sponsor CRAs are not qualified by education, training and experience to be able to determine if a CT scan/MRI for instance, meets an appropriate standard of a regulator.  Sponsor provided systems (ePRO, econsent) would be the responsibility of the sponsor.  Please consider to change as described. |  |
| 364-386 (Section 4.4 Source data) |  | **Comment:** The definition of eSource Data as *“the first obtainable permanent data from an electronic data generation/capture should be considered and defined as the electronic source data.”* can in many instances be rendered unpractical and invaluable both for data provider, investigator and sponsor and as well in many cases won’t secure the regeneration of outcome for the final result. The concurrent more intelligent data capture methods (e.g., specific motion detections, intelligent image analysis) requires a dedicated analysis step performed by a third party not being the sponsor or investigator.  In other methods of data capture e.g., Patient Reported Outcomes we accept that source data is an understandable format e.g., answers to a questionnaire. How come we can’t accept this to be the same with novel methods of data capture as long as the methods have gone through the extensive validation requirements we have for the data capture mechanisms? |  |
| 367, 613 |  | **Comment:** What is the difference between source data files vs source documents? Are files and electronic documents regarded equivalent in this document?  Please add a clarification/ definition. |  |
| 369-370 |  | **Comment:** Clarification is required regarding in which document the source data be defined and whether this document should be held by the vendor or the sponsor. |  |
| 370 |  | **Comment:** Proposed change regarding ‘*retained*’:  **Proposed change (if any):**  “It is important to ensure that the true source data list is understood, defined and securely retained.” |  |
| 371-372 |  | **Comment:** The identification of the location of source documents and associated source data they contain at all points within the data capture processis the principal investigator’s responsibility (see comment to 312-314).  Please clarify. |  |
| 373 |  | **Comment:** It is not clear if this means that the box labelled "Image" can be considered source data, or if the box labelled "Data" is the source data.  Please clarify. |  |
| 373-375 |  | **Comment:** We would suggest to clarify the wording.  It is not clear in figure 1, what should be considered as source data and therefore be retained. This needs to be crystal-clear to readers who are not so familiar with these ideas. It would be helpful to indicate whether it is being suggested that the Data (Step 1) is the source or whether the Image (Step 2) is the source. Or perhaps there are times when either could be deemed source, in which case this should be explained.  **Proposed change (if any):**  “Below is an example (figure 1) of a situation where the true source data (e.g. imaging~~, but could also 374 relate to information from a wearable~~) is often not used for source data verification, or ~~it~~ is not retained ~~ensured that it is retained~~”  On Figure 1, it could help to make the point to add the following:  **Addition**  Please add “true Source data” in the respective blue boxes in the example figure. We would recommend combining the label and associated descriptions into one box to make the association more obvious.  In the lowest right box of Figure 1, the term “data” is a bit unclear. Please change “data” to “eCRF data”. |  |
| 374 |  | **Comment**: *“wearable”* should be included in the definitions and include examples of what wearables are. |  |
| 375-378 |  | **Comment:** Clarification is requested as the extent of source data verification that would be required as well as what would be considered to be the first obtainable permanent data. |  |
| 377-383 |  | **Comment:** In case of not human readable image, which is transcribed into a simple report with results, how is the validation performed for the non-readable image to be validated? What will be checked by the sponsor at the site? |  |
| 378-379 |  | **Comment:**  378: The statement relates to the box with *'data'* in figure 1 as *'source data'*, but this information is not human-readable (A\*\*\*L\*\*\*COA++).  379: The statement relates to the box with *'image'* in figure 1 as *'source data'* as this is the instance where full ALCOA++ principles hold true.  Further clarification is needed to clearly define source data in light of ALCOA++ principles, which also could be used in source data verification (by humans). The scenario suggests that the earliest practically retainable record (i.e., the reported results) could be considered a source document for the purposes of source data verification – could this be clarified?  Please add a clarification/ definition. |  |
| 378-383 |  | **Comment:** It is unclear where the definition of *“source data”* should be captured in the clinical trial documentation. Clarification would be helpful.  In the example below -- the actual first recorded data on the subject's mobile phone or wearable device is no longer considered the "source" nor "raw" data - but only that data that actually makes it to the central server. In this case, why should a lab have to consider the data collected by a portable integrator to be the raw, source data if it is not uploaded yet to a central server or processor? The extracted features from the raw data could be a better choice of source data level.  Please ensure consistency in examples with what is proposed in the guideline.  **Proposed change (if any):**  “the first obtainable permanent data from an electronic data generation/capture should be considered and defined as the electronic source data. For data collected through sensors, the first level of legible data, (i.e., not the raw data but for example the extracted features) should be considered and defined as the electronic source data.” |  |
| 379-382 |  | **Comment:** We would recommend referring to ALCOA ++ for consistency throughout the document.  **Proposed change (if any):**  “This process should be validated to ensure that the source data generated/captured is representative of the original observation and should contain metadata, including audit trail, to ensure data is attributable, legible, complete, original, accurate, contemporaneous, consistent, enduring, and available (see minimum requirements for electronic source data).”  Alternatively, please indicate that the data must meet ALCOA++ principles. |  |
| 383 |  | **Comment:** Some clarity is required around this expectation to capture the logical location within metadata. Logical location could also imply location of the data capturing device within a network bus/network segment which may not always be unique for a device. We recommend the following wording to ensure logical location can be clearly attributed to the device capturing the source data.  **Proposed change (if any):**  “The logical location unique to the device where the source data is first obtained (e.g., Device ID, Serial Number, etc.) should be part of the metadata.” |  |
| 384 Figure 2 |  | **Comment:** Figure 2 requires clarification if the investigator should receive identifiable data and only the sponsor should receive pseudonymized data. Figure 2 currently indicates both investigator and sponsor receiving data from the Central server which is pseudonymized data.  Please remove ambiguity and clarify. |  |
| 384 |  | **Comment:** The definition of electronic source data appears discrepant. Line 384 indicates once data is transferred to a server, it is considered source data. Line 1380 indicates data stored in a device is source data.  In the image below line 384 the data on electronic device are defined *“Temporary storage until …"* and the data on the central server are defined as *“source data”*, while in line 1380 the data on electronic device are defined as *“source data”* and the data on the central server are defined as *“certified copy”*.  Edit may be required for clarification. |  |
| 384 |  | **Comment:** The diagram is a big simplification in the case of data extracted from wearables. It is not clear if it refers to the raw data, to the extracted features, or to any step in between.  We would suggest to clarify the diagram on Figure 2 for the example of sensor-collected data as its use in clinical trials is increasing. In case of wearable device, the data on electronic device is considered as source.  What should be considered for the trial - is it data from electronic device or data from a central server? What validation documents would be required in case of each wearable device provided to the subject?  **Proposed change (if any):**  On Figure 2, “Sponsor receives the certified copy of the data and metadata as dynamic files and undertakes data analysis for the trial.”  *\*Delete the space between meta and data.* |  |
| 385 |  | **Comment:** This example seems to be written with a specific use case in mind (i.e., three parties involved; sponsor, investigator, and some unspecified third party owning a central server); the central server could be with the investigator.  Please clarify that this is a specific use case with a third party central server, and that the central server may be owned by the investigator; in such a case, no certified copy to the investigator is required. |  |
| 387 |  | **Comment:** Since these principles are foundational, this section should be at the top of the list in the glossary.  **Proposed change (if any):**  Please consider relocating the ALCOA principles to the beginning of the document. |  |
| 387 Section 4.5. |  | **Comment:** Like with CSV and the definitions, is it necessary to recreate ALCOA ++ as this is a well-understood term. |  |
| 389 |  | **Comment:** Should the data also be clearly attributable to a particular research subject in the clinical trial? For example, which subject does the data apply to? |  |
| 390 |  | **Comment:** *“Data should be attributable to the person generating the data.”* This is unclear and open to interpretation. For example, a heart monitor running over multiple shifts -- the machine itself is generating the data, not a person. Or is it considered that the person to whom the monitor is attached would be the generator? Or is it the person who starts the machine?  Please clarify what the data should be attributable to. |  |
| 390 |  | **Comment:** It is suggested that the following text be deleted: *“Based on the criticality of the data”*. All data irrespective of the criticality should be traceable to the system/device in which the data was generated/capture.  **Proposed change (if any):**  “~~Based on the criticality of the data it~~ It should also be traceable to the system/device, in which the data were generated/captured.” |  |
| 394-396 |  | **Comment:** The definition of legible is missing some of the common industry definition.  **Proposed change (if any):**  **Addition**  Please add the following to the definition of Legible:  “All data recorded must be readable and permanent. This includes maintenance of the data throughout its life cycle i.e., storage in a human-readable form together with the metadata recorded supporting the electronic record.” |  |
| 403-406 |  | **Comment:** This seems to imply that it is necessary to maintain the initial dynamic state in which the information was originally captured, which is not feasible. Clarification is required.  *“Remain in that state”* needs clarifying in terms of functionally equivalent or keeping exact dynamic nature of original system. We would suggest providing additional text on functionality to keep, e.g., Ability to search; recalculate using original algorithm or method (with minor changes to parameters) - often called ‘what if review’. |  |
| 418-419 |  | **Comment:** We would suggest adding that some reduction in the fidelity of metadata is allowable (especially if transferring data and records to another system); but this should be based upon a documented risk due to importance to the study outcome or patient safety considerations. |  |
| 423 |  | **Comment:** Proposed change regarding “*by the use of*”.  **Proposed change (if any):**  “to minimise the risk of contradictions e.g. using ~~by the use of~~ standardisation” |  |
| 430 |  | **Comment:** Please make the current wording more precise.  **Proposed change (if any):**  “Data should be accessible ~~stored~~ throughout the data life cycle, ~~at all times~~ in a controlled manner ~~order to be~~ that is readily available for review when needed.” |  |
| 435-463 |  | **Comment:** Section 4.6 focuses on risksbut does not address the concept of criticality. The term *“criticality”* is neither defined nor used in the section. It would be useful to have a definition and use similar to the one by MHRA (criticality of data, risk to data). |  |
| 436-439 |  | **Comment:** ICH E6 (R2) section 5.0.2 has a slightly different definition: *“The sponsor should identify risks to critical trial processes and data. Risks should be considered at both the system level (e.g., standard operating procedures, computerized systems, and personnel) and clinical trial level (e.g., trial design, data collection, and informed consent process).”* |  |
| 437 |  | **Comment:** To provide more clarity, please add *“core”* system level. Also, it would be great to provide more clarity around what *“computer systems and staff”* refer to since the paragraph is about system and trial level risk but then references computer systems. |  |
| 442 |  | **Comment:** We would suggest clarifying that mitigation actions are not limited to the examples provided.  **Proposed change (if any):**  “mitigating actions include but are not limited to revised system design” |  |
| 447-448 |  | **Comment:** *“The complicity between each component”* – Do you mean “*interfaces”*? (to be aligned with line 568)  **Proposed change (if any):**  “The interdependency ~~complicity~~ between ~~each~~ components should be taken into consideration.” |  |
| 449 |  | **Comment:** The term *“reliable”* is unclear in terms of its meaning.  Delete *“approved”* as *“in the context of a clinical trial”* should be sufficient.  **Proposed change (if any):**  “All data collected in the context of ~~an approved~~ a clinical trial should ~~be reliable~~ meet ALCOA++.” |  |
| 451 |  | **Comment:** Remove *“are”.*  **Proposed change (if any):**  “are generated, ~~are~~ recorded, processed” |  |
| 459-460 |  | **Comment:** This sentence seems out of place and redundant based on the previous paragraphs.  **Proposed change (if any):**  Please remove the following sentence:  “~~The identification of the most effective and efficient risk-based control, including periodic review of the data and metadata can be determined and implemented.~~” |  |
| 464 |  | **Comment:** Is it acceptable to have this information in multiple records and not in the protocol? Specifying this in the protocol could be too specific and subject to too many changes for a protocol. The protocol could cover the types of data captured (e.g., digital vs manual), and another document referenced in the protocol could capture the specifics. This document could be the data source location document, the data management plan, etc.  For “*or procedures*”, does this imply that specific operational considerations would be in a protocol or are there cases where those specifics would be more appropriately outlined in a “work instruction” or “job aid” to keep the protocol succinct and manageable? For example, the specifics of which buttons to push in which sequence on a wearable.  More generally, the proposed sentence is too detailed and contrary to the concept of protocol simplification.  We would suggest adding *“duration”* for data capture in clinical trials, especially for data collected from wearable devices.  **Proposed change (if any):**  “The approved clinical trial protocol should specify which data is to be generated/captured by whom and when (including duration, for wearable devices)and which tools (i.e., systems, templates, devices, etc.) or procedures are to be used. The provided information could also be provided in another protocol referenced document.” |  |
| 466-469 |  | **Comment:** The impact of this statement will likely mean that the protocol will just list ALL data as source data, to be safe from any non-compliance.  It should be clarified whether the expectation that data being collected in tools like eCRFs, ePRO, etc. be identified down to the specific data field level (i.e., date, time, activity level, mood) or if it is acceptable to identify the type of data (i.e., Patient daily diary entries).  Some CROs provide a Source Data Agreement which clearly indicates direct data entry in eCRF, involvement of a paper source, etc. It would be more practical to refer to such a Source Data Agreement in the protocol to cover source data rather than indicating this in the protocol for each data type with the risk of missing something.  This seems to contradict the example in line 384 (Figure 2), which is not source data until it is uploaded in a server.  It also appears to contradict lines 1380-1382: *“The data saved in the device are considered source data. After the data are transferred to the server via a validated procedure, the data on the server are considered a certified copy.”*  **Proposed change (if any):**  “All source data must be defined in the protocol ~~The protocol should identify any data to be recorded directly into the eCRFs and considered to be source data~~ (ICH-GCP 6.4.9), and all defined source data must be captured appropriately, e.g., via eCRF, ePRO, EDC. This is equally applicable to other specific data collection systems, such as eCOA ~~PRO~~. Data directly captured in these tools without prior identification in the protocol to be source data not captured appropriately is considered as GCP-noncompliance ~~noncompliant~~.” |  |
| 468-469 |  | **Comment:** Clarification is required as to whether this should specify patient data. |  |
| 474-478 |  | **Comment:** These paragraphs seem out of place.  **Proposed change (if any):**  Please place the following paragraph up to line 470 (prior to the preceding paragraph):  “The sponsor and investigator should maintain a record of the location(s) of their respective essential documents including source documents (ICH-GCP 8.1). Investigators should document source data consistently in accordance with the source data location list. The source data and their respective capture methods should be clearly defined prior to the recruitment of the trial participants.” |  |
| 479-482 |  | **Comment:** Electronic Data flow diagrams are typically part of individual computerised system design documents. Since multiple computer systems may be used during the conduct of a clinical trial, it is important to depict the overall data flow between these systems for any particular trial. Therefore, it is suggested the following change to emphasise the need for trial-specific data flow diagrams.  Is the description intended to exist somewhere or to be specifically included in the protocol? If the latter, then this should be specified.  Section 4.7 - Is this detailed diagram linked to data flow? See refence to ISPE GAMP on data flow principles and wording used for Data Flow diagrams. Please provide clarification on the Detailed Diagram to harmonize the wording with GAMP principles.  A specific reference to GCP or other clinical standard should be added to support this statement.  Is a detailed diagram / data flow required for each source of electronic data? Would text descriptions / Data Transfer Agreements be acceptable?  **Proposed change (if any):**  “A detailed diagram and/or description of the transmission of electronic data expected during the conduct of the clinical trial should be available.” |  |
| 483 |  | **Comment:** *“data management plan (DMP) is strongly encouraged”* Do you mean data flow or system overview, which are two different documents produced in the context of the CSV?  The use of Data Management Plan should be mandated and not optional, in consistency with GCP requirements. |  |
| 484-485 |  | **Comment:** The definition of data seems to be outside the remit of GCP regulations. We may capture other data for planning/ performance/ financial reasons (e.g., delivery/ logistics KPIs) which are not relevant to the conduct of the trial or protocol.  Clarification is requested as to whether this should specify patient data. It should also be clarified whether data included in a transfer (i.e., check sums, date and time stamps) are required to be captured in the protocol.  **Proposed change (if any):**  “Any data defined in the protocol that is not generated/captured and/or transferred to the sponsor or CRO ~~that is not stated in the protocol or related documents~~ is considered GCP-noncompliant.” |  |
| 486-490 |  | **Comment:** We suggest that this is better suited in the preamble as it seems out of place in the current section. |  |
| 487 |  | **Comment:** *“electronic data collection”* is not correct.  **Proposed change (if any):**  “the use of electronic data capture ~~collection~~ (EDC) tools” |  |
| 488 |  | **Comment:** Clarification is required as to which standards are expected for study protocol design within EDC systems/tools. In some instances, EU inspectors have expected complete validation/qualification to be performed for every study protocol designed or configured within the EDC system/platform in addition to the validation of the underlying EDC system/platform. It is recommended that EMA considers providing some guidelines/ standards (e.g., configurations documented and verified against approved study protocol, edit check testing documented, etc.) around expectations for validation of study protocol within EDC systems. |  |
| 489 |  | **Comment:** Under *“attributability”*, we recommend allowing the use of a scribe to record activity on behalf of another operator. This is in alignment with MHRA GXP Data Integrity Guidance and Definitions and WHO Annex 5 Guidance on good data and record management practices. |  |
| 491-520, Section 4.8 |  | **Comment:** We would suggest specifying what systems (closed or open systems) the wearable device (long-term passive digital data collection from wearable devices) should use and how electronic signatures or other approaches should be used for identification purposes. |  |
| 492, 500 |  | **Comment:** We would propose amending the text as follows as it is missing a requirement for electronic signature.  **Proposed change (if any):**  Line 492: “Whenever an electronic signature is used within a clinical trial to replace a wet-ink signature required by GCP, the electronic signature functionality should meet the expectations stated below regarding authentication, non-repudiation, unbreakable link, ~~and~~ timestamp of the signature and the reason for the signature"  Line 500: “4) provide a *timestamp*, i.e., that the date, time and time zone when the signature was applied is recorded, 5) reason for Signature.” |  |
| 492-520, Section 4.8 |  | **Comment:** Electronic signatures – the guideline misses to address different use cases, there must be a huge difference if the signature is for patients and investigators. If there is an open system, i.e., they don’t know each other, should both parties use personal qualified signatures (eIDAS) or only the patient? Also, if for example a CRA is performing remote monitoring and is never meeting the investigator, hence they do not know each other, is this regarded an open system and hence needs the QES? We need more use cases in the section – ICF signatures cannot be treated the same way as signing of delegation log. Regarding QES, it should be discussed whether Advanced Electronic Signatures couldn’t be sufficient. QES implies that the signature would have to use a trusted provider and call a video agent to confirm identity. This creates a very cumbersome method for signing an ICF electronically. |  |
| 499 |  | **Comment:** Please clarify the intent of #3 – the following proposed modification is suggested.  **Proposed change (if any):**  “3) ensure an unbreakable link between the electronic record and its signature, i.e. that the contents of a signed (approved) version of a record cannot later be changed by anyone without automatically being rendered visibly ~~un-signed (unapproved)~~ invalid and/or identified that the record has been modified. If the content of a signed electronic record is changed, the record should be prompted to be re-signed following the change.” |  |
| 503 |  | **Comment:** Open and Closed should be defined within the context of this section as other regulations (21 CFR Part 11) have definitions that may not match, causing confusion. |  |
| 504 |  | **Comment:** Is it necessary to indicate closed systems are the majority of systems used by sponsors? It is possible that this could change over time as technologies evolve particularly for supporting systems and the increased use of SaaS and outsourcing. We would suggest this wording is not necessary. |  |
| 505 |  | **Comment:** Clarification is required as to whether *“knows”* should be replaced with *“is responsible for maintaining”* the identity of all users and signatories. *“Knows”* is not definitive as to the expectation that the system owner ought to know the identity of all users and signatories.  **Proposed change (if any):**  “the system owner is responsible for maintaining ~~knows~~ the identity of all users and signatories and has full control over these.” |  |
| 510-512 |  | **Comment:** This requirement is only applicable in the EU. It would require qualified signatures according to eIDAS for any activities involving open systems and actors from third countries. This is not practicable on a global scale where most relevant countries would accept signatures according to 21 part 11 FDA requirements. Therefore, an authentication via PIN and e-mail (any two-factor authentication) should be acceptable. It is more important that individuals agree to the usage of an electronic signature and know each other.  Clarification is required as to who should have the accountability for ensuring that open system signatures comply with EU Regulation 910/2014 i.e., the sponsor receiving the signed documents or the site/investigator using an open system to sign documents. |  |
| 513-517 |  | **Comment:** The notion of a checksum (hash code) calculated for the electronic record and printed by the system on the signature page is not feasible for many systems. We suggest removing the specific mention of an example with hash codes.  In addition, in case of hybrid signatures, another commonly observed scenario is one where multiple signatures are captured, some electronically and some on paper (wet-ink). Additional guidance (as proposed below) is recommended for such scenarios.  **Proposed change (if any):**  “A special case of electronic signatures is *hybrid electronic signatures*, where electronic records in a computerised system are signed using wet-ink signatures on paper. In this case, it follows from the above that there should be sufficient controls for hybrid systems in place so that ~~an unbreakable~~ a clear link between the electronic record in the computerised system and the signature page on paper is maintained ~~e.g. by means of a checksum (hash code) calculated for the electronic record and printed by the system on the signature page~~.In situations where multiple signers need to sign a document, some electronically and some on paper (wet-ink), both documents, i.e., electronic and paper form, should be retained to preserve the integrity of the document and the signatures.” |  |
| 518-519 |  | **Comment:** The statement assumes biometrics replaces e-signature (i.e., instead). Biometrics can be used to record/input e-signature.  Biometrics are not e-signatures and cannot be used as e-signatures. Biometrics are a control used to authenticate someone who is applying an e-signature. One cannot "use biometrics instead of signature". One is a method for application, the other is the subject of the application.  **Proposed change (if any):**  “If using biometrics to record~~instead of~~ signature or e-signature, investigator and sponsor should ensure that these fulfil the above-mentioned requirements and local legal requirements.” |  |
| 524-529 |  | **Comment:** *“The requirements of Regulation (EU) 2016/679 (General Data Protection Regulation) on the protection of individuals with regard to the processing of personal data and on the free movement of such data should be followed except when specific requirements are implemented for clinical trials e.g. that a trial participant does not have the right to be forgotten (and consequently data deleted) as this would cause bias to e.g. safety data (Regulation 536/2014 recital 76). Trial participants should not be asked to waive their rights by informed consent processes (ICH-GCP section 4.8.4.).”*  This passage needs to be rephrased (positive statements instead of negative ones?) in order to avoid misunderstandings.  Statements seem to contradict each other - please clarify: data privacy can be limited during participation in clinical trials, but investigators/sponsors should not make participants aware and ask for consent? Shouldn’t the participant explicitly be made aware that in case of clinical trial participation, data privacy rights might be limited in the sense that data cannot be revoked or deleted?  Given that there may be justified reasons for not implementing parts of GDPR (e.g., right to be forgotten due to compensation requirements in 536/2014), these must be explained in the informed consent, and participants must agree that they lose this right because there is a superseding regulation. Trial participants should be informed of any GDPR rights that may not apply due to their participation in a trial via informed consent processes; although this seems to contradict ICH-GCP section 4.8.4.  Please clarify/resolve the apparent conflict between GDPR rights that must be waived to participate in a trial and the ICH-GCP 4.8.4 clause preventing this. |  |
| 530 & 532 |  | **Comment:** Please clarify “*Union*”.  **Proposed change (if any):**  “In accordance with European Union data protection legislation, the location of personal data processed (both at rest and in transit) must be within the EU/EEA. If personal data is transferred to a third country or international organisation, such data transfer must comply with applicable European Union data protection.” |  |
| 533-536 |  | **Comment:** Duplication of GDPR is not required.  **Proposed change (if any):**  Please remove this duplicative text:  “~~In summary, this means that the transfer must be either carried out on the basis of an adequacy decision (Article 45 of GDPR, Article 47 of EUDPR), otherwise the transfer must be subject to appropriate safeguards (as listed in Article 46 of GDPR or Article 48 of EUDPR) or the transfer may take only if a derogation for specific situations apply (under Article 49 of GDPR or Article 50 of EUDPR).~~” |  |
| 535 |  | **Comment:** *“take only”* is not correct, perhaps add *“place”*.  **Proposed change (if any):**  “the transfer may take place only if” |  |
| 537 |  | **Comment:** For Section 4.10, Validation of Systems, greater specificity/clarity is required regarding requirements related to ownership/responsibility of the documentation e.g., system validation.  It would be impractical for sponsors (not CROs) to manage validation for every SaaS application, especially as this is partially already contracted to a vendor.  Please add verbiage explaining the concept of risk-based validation. |  |
| 538-541 |  | **Comment:** Under Scope (line 294), it is stated that *“The approach towards computerised systems and medical devices used in clinical practice […] should be risk proportionate”*. Line 538 could be understood as *“All computerised systems used within a clinical trial need to be validated.”*. This is a contradiction.  **Proposed change (if any)**  “All computerised systems used within a clinical trial should be subject to processes that confirm that the specified requirements of a computerised system are consistently fulfilled and that the system is fit for purpose. An approach of validation should be risk-proportionate or risk-based to ensure accuracy, reliability and consistent intended performance, from design until decommissioning of the system or transition to a new system.” |  |
| 542 |  | **Comment:** Why are the processes used for validation decided upon by the system owner? The validation processes are owned by Quality or Compliance teams of an organization.  **Proposed change (if any):**  “The processes used for the validation should be decided based on the risk, criticality and intended use of the system ~~upon~~ by the system owner (e.g. sponsors, investigators, technical facilities) and described, as applicable.” |  |
| 544 |  | **Comment:** We would prefer referring to *"records"* throughout instead of *"documentation"* as *"documentation"* implies non-value adding paperwork that is done separately from the actual work. Paper-driven mindsets must be replaced with data and record-driven thinking. (not all instances where this should be changed would be listed).  **Proposed change (if any):**  Please review any mention of *“documents”* and replace with a term more relevant to today’s digital landscape. |  |
| 546-549 |  | **Comment:** For systems which are developed by third parties (e.g., vendors) clarification is required as to whether it is acceptable to maintain development documentation created by the vendor, at the vendor location, provided the sponsor has access to the documentation when needed or if the sponsor is required to retain and store this type of documentation in-house. |  |
| 553 |  | **Comment:** We recommend changing the term *“dose calculation”* to *“drug dispensing”* when referring to IRT, since that is the most adequate term for the activities executed using such solutions.  **Proposed change (if any):**  “for example, eligibility criteria questions in an eCRF, randomisation strata and dose dispensing ~~calculations~~ in an IRT system.” |  |
| 555, 556 |  | **Comment:** We would propose amending section 4.11 heading.  We would propose to clarify that the access needs to be *“Read-Only”* (Guest/Auditor Account).  If direct (read only) access is not possible for a system, it should be clarified if a driver can be provided in these situations.  There should be clear guidance indicating to which type of computerised systems direct access by inspectors is required during inspections, i.e., TMFs, eCRF, ePRO, eCOA, etc.  We would suggest defining how long after a system is decommissioned it should be available to access (e.g., less than 12 months). The current statement can imply an indefinite timeline. It means keeping the database live for extended periods of time, and maybe even unlocking at the time of inspection. It may also mean keeping the hardware, software licenses and operating systems running, which in times of frequent technology changes is impossible to do or not even supported by the original provider.  Can the expectation of this direct data access (post system decommission) be explained further? For instance, if the system software is not the same as before, but still data is humanly readable, is it acceptable? This section should allow for the possibility of a risk-based approach to access data over time.  We would suggest adding a condition that if direct access cannot be provided, access to the data needs to be ensured. For some legacy systems, it may not be possible to establish direct access.  **Proposed change (if any):**  Section heading 4.11.: “Direct access to ~~computerised systems~~ data”  “All relevant data managed with computerised systems should be readily available and directly accessible (this requires authentication of the individual using validated and secure methods ~~a unique username and password~~) upon request by monitors, auditors and inspectors of regulatory authorities. If a computerised system is decommissioned, direct access (with authentication of the individual using validated and secure methods ~~personal username and password~~) with a “Read-Only” account to the data in the archived format should be still ensured (see section 6.10~~11~~). Inspectors will be expected to have organisation specific training for access to electronic systems. The training should be efficient and useful in ensuring competence in using the system.”  Alternatively, re-phrase as follows:  “Sponsors should have a process of granting access to the computerized systems during the course of inspection. In case of a scenario wherein access cannot be provided, a well-established process should be present as a workaround towards the same.” |  |
| 555-559 Section 4.11 – 878- 891 6.11 decommission |  | **Comment:** Is the vendor supplying the system obliged to keep and maintain the data after decommissioning? Restoring of database including dynamic functionalities and all relevant metadata is a problem. Does this mean that the actual platforms used should be accessible after involvement from vendors? |  |
| 563-569 |  | **Comment:** Does section 5.1 refer to a Computerized system Inventory List as known from the GMP area? A requirement for a System Inventory List has never been clearly formulated by the EMA, however it is often asked for during inspections.  Please specify if that information shall be documented in a System Inventory List and which information shall be stored there. |  |
| 563 |  | **Comment:**  The description of end-to-end dataflow (within and/or between multiple computerised systems/databases) is missing.  **Proposed change (if any):**  Section 5.1 heading: “Keeping a description of computerised systemsandend-to end dataflow (within and/or between multiple computerised systems/databases)” |  |
| 564-566 |  | **Comment:** In situations where cloud service providers are used to store clinical data, getting the exact physical location of the servers from providers is always a challenge for the industry for security reasons. It is recommended that additional guidance be included as suggested below, for physical location of the servers. Clarification is required as to whether it is acceptable for the sponsor to assess the provider to verify adequate controls and oversight of their activities and confirm that such a list is maintained even though not made available to the sponsor. If this is not acceptable, a suggested alternative approach would be for only high-level details of the location to be shared with the sponsor such as geographic region, country, state.  A server will most likely consist of a virtual machine within a data centre. Whilst the geographic location of the data centre can be determined, the exact hardware on which the virtual machine is active will not be available to the Sponsor and may change during the course of the study due to fail-over activities in case of system failure.  It should be clear that the location of data on a specifically named server is not always feasible (e.g., cloud-based environment) and not an expectation.  Please specify what clinical standard/GCP section is this requirement of list referring to: *“used in a clinical trial”* is too detailed/unrealistic down to a study level. |  |
| 567 |  | **Comment:** Please clarify what is meant by *"methods used"* and *"security measures"* as this context may be misinterpreted.  “extent of computerization” and the overall expectation is not clear. The requirement in general should be met by system lifecycle deliverables.  **Proposed change (if any):**  “Where multiple computerised systems/databases are used, design specifications which should state the end-to-end system data flow, supporting business processes, and the interfaces/ integrations ~~a clear overview~~ should be available ~~so the extent of computerisation can be understood~~.” |  |
| 570 |  | **Comment:** Greater specificity/clarity is required regarding requirements for ownership/reporting of documents. |  |
| 573-584 |  | **Comment:** It is suggested that the scope of training requirements be defined for inspectors accessing systems as the scope currently limits this to those *“involved in conducting a clinical trial”*.  Inspectors often request waivers for this foundational expectation. For this reason, we recommend that the Agency indicates if it is proper to grant access to inspectors without evidence of minimum training on the sponsors’ systems and its stance on granting training waivers for regulatory inspectors. |  |
| 573-584 Section 5.3 |  | **Comment:** *“considerations should be considered”* does not sound correct.  Training of trial participants should be kept to a minimum and instead the design should follow patient-centric principles making the system so intuitive that training is not relevant.  Training of trial participants does not appear to be covered in section 5.3.  **Proposed change (if any):**  “Special considerations should be given to ~~considered regarding~~ training of trial participants when (or where) they are users.”  Please update the reference or add the expectations in section 5.3. |  |
| 579-580 |  | **Comment:** *“Relevant aspects”* is a broad description and may be interpreted in a variety of ways.  Clarification is required as to whether this refers to training of vendors or third parties from a technical development aspect or if it is the intent also to include training and knowledge on applicable GxP legislation as well (e.g., ICH E6).  Please add more specific information about the level of training needed of the legislation. |  |
| 583-584 |  | **Comment:** Clarification is required as to whether training performed by sponsor/vendors employees must be documented in the site file/sponsor TMF.  This will have an important impact; this requires that all the training records for all the "back office" people (e.g., IT developers/QA eCompliance/ISRM/Data Privacy) involved in system implementation and operation need to be added to every TMF. This does not seem useful.  Please clarify what records must be added to TMF, and what records must be available but not necessarily attached to the TMF.  Are / should training records of trial participants using data collection devices be covered by eConsent? Is a separate training record of participants for devices used in clinical trials necessary?  Please clarify.  **Proposed change (if any):**  “All training should be documented, and the records retained in the appropriate part of the investigator site file~~/sponsor TMF~~and made available to the sponsor on request.” |  |
| 588 |  | **Comment:** Deliberate data changes are needed.  **Proposed change (if any):**  “~~deliberate~~ malicious or unwanted data changes and maintain blinding of the treatment allocation where applicable.” |  |
| 589-590 |  | **Comment:** Clarification is required as to which type of system checks should be used e.g., automatic system checks to verify correct log in information is used (i.e., ID/Password) and prevent unauthorised access, periodic checks of the individuals (users listing) who have been granted access to the system to confirm they still should have access or a combination of both. |  |
| 590 |  | **Comment:** The example is very limited.  **Proposed change (if any):**  “appropriate permissions ~~(e.g. ability to enter or make changes to data)~~.” |  |
| 595 |  | **Comment:**  In the context of this section, should the reference be *“handling of security breaches”* instead of *“handling of serious breaches”*?  **Proposed change (if any):**  “handling of security ~~serious~~ breaches.” |  |
| 596 |  | **Comment:** Does the scope also cover portals for supplying information from the sites to the sponsor, e.g., medical records for the purpose of remote monitoring? If so, please consider adding. |  |
| 597 |  | **Comment:** Most, if not all, of this section is somewhat redundant to section 4.  Please consider removing some sub-sections or streamlining this section, in particular section 6 and sub-section 6.1. |  |
| 598-601 |  | **Comment:** Consideration should be given to an exception for data such as high frequency data that comes from mobile devices and without an algorithm to interpret it is meaningless to the investigator. Having access to billions of records is both meaningless and wasteful, so should be avoided. Access to meaningful data is what is important here. |  |
| 599 |  | **Comment:** Clarification on the first sentence is required. The electronic source data cannot be accessed for blinded studies without compromising the confidentiality of participants and their identities or the integrity of the trial. |  |
| 604 |  | **Comment:** “*in a timely manner”* should be replaced with *“contemporaneously”* in keeping with ALCOA descriptions.  **Proposed change (if any):**  “All pertinent observations should be documented contemporaneously ~~in a timely manner~~.” |  |
| 608-609 |  | **Comment:** The use of E-Systems is not mandated, therefore it is not mandatory to transcribe from paper to electronic media - please replace *“need to”* with *“may”*.  **Proposed change (if any):**  “~~need to~~ may be transcribed” |  |
| 610 |  | **Comment:**  More clarification is needed on risk-based methods for manual transcriptions. What is meant by risk-based methods in terms of transcription?  **Proposed change (if any):**  “risk-based methods should be implemented and documented to verify ~~ensure~~ the quality of the transcribed data” |  |
| 611 |  | **Comment:** There are two periods (..) at the end of the sentence.  **Proposed change (if any):**  “(e.g. double data entry and/or data monitoring).~~.~~”  *\* Delete one of two periods.* |  |
| 612-624 |  | **Comment:** ICH E6 (R2) Section 8.1 states: *“The sponsor should ensure that the investigator has control of and continuous access to the CRF data reported to the sponsor. The sponsor should not have exclusive control of those data.”*  Clarity is needed to verify if all third party data streams need to include audit trail / metadata for each data transfer. |  |
| 613-618 |  | **Comment:** Clarification is required as to whether, should a need arise for a data transfer to occur outside of a pre-defined period, it is acceptable to document this need, what was transferred and rationale for the transfer in a note to file in the study files. There are occasions where and unscheduled data transfer needs to occur due to regulatory requests or potential safety assessment needs.  Please clarify why this is necessary as ad hoc data transfers are often required for final data reconciliation efforts at times such as interim analyses and Database Locks. |  |
| 616 |  | **Comment:** Please correct the grammar.  **Proposed change (if any):**  “secured/encrypted in a way which precludes disclosure of” |  |
| 618 |  | **Comment:** Clarification is required as this section may be misinterpreted. Please confirm *“pre-specified"* means before transfer and not before trial start.  Additionally, clarification is required regarding what is in scope for data transfer.  **Proposed change (if any):**  “All transfers that are needed during the conduct of a clinical trial need to be described in a transfer plan or equivalent document ~~pre-specified~~.” |  |
| 619-620 |  | **Comment:** We recommend that the Agency enables parties to establish their own risk-based approaches for data transfers, in alignment with complexity, past experiences, criticality of the data, and trial milestones.  The justification for mandating when a specific data transfer process be established is unclear. It is perfectly reasonable that a trial is started with a certain transfer process, then a year later a better transfer process is identified, which is then validated and applied to the ongoing trial. This is part of continuous improvement. As stated, this text implies that once a trial starts with a certain transfer process, this cannot be changed.  **Proposed change (if any):**  “~~Qualification/validation of transfer should include appropriate challenging test sets and ensure that the process is available and functioning at clinical trial start~~ Test transfers should be risk-based and executed prior to first production transfer, to confirm the qualification/validation status of the transfer (e.g., to enable ongoing sponsor review of diary data, lab data or adverse events by safety committees).” |  |
| 621 |  | **Comment:** We would propose removing the terms *“transcribed or extracted”*. Data which is transcribed from one system and put in a file is not the same as data transfer. This section is about *“transfers in and between systems”* so the term *“transcribed or extracted”* appears out of place. Transcription would be covered by other means to protect data integrity such as a certified copy.  Can *“continuously accessible”* be defined and/or better clarified?  **Proposed change (if any):**  “Data ~~transcribed or extracted and~~ transferred from electronic sources and their associated audit trail should be continuously accessible (according to delegated roles and corresponding access rights) by the sponsor for ongoing review and by the investigator for the entire clinical trial and retention period (ICH-GCP 8.1).” |  |
| 625 |  | **Comment:** Please update the term *"transfer"* with *"migration"* to be consistent with the term as defined in Section 6.9.  **Proposed change (if any):**  “~~Transfer~~ Migration of source data and records where the original data or file is not maintained is a critical process and ~~appropriate considerations are expected in order~~ should follow ALCOA ++ requirements to prevent loss of data and metadata.” |  |
| 630-631 |  | **Comment:** It is not clear what a *“special”* questionnaire refers to, or why the following statement appears to be specific to PRO data:  *“Where treatment-related pertinent information is captured first in a direct data capture tool such as a trial participant diary, a PRO Guideline on computerised systems and electronic data in clinical trials form or a special questionnaire, a written procedure should exist to transfer or transcribe information into the medical record, when relevant”*.  Ownership of the mentioned written procedure is not clear. Please specify the written procedure of site level or sponsor level.  Please clarify the statement and refer to eCOA more broadly. |  |
| 633-634 |  | **Comment:** Why is there the need to link direct data capture tools to the EDC system used for the trial? It could also be connected directly to a Clinical Data Repository or other solutions.  We would suggest to add that the information concerning the individual device’s metadata does not have to be maintained by the sponsor but can also be maintained by the service provider as this information in some events can create a possible way for the sponsor to distinguish certain personal information on the subject e.g., if they are using their own mobile phone for data capture.  **Proposed change (if any):**  “Direct data capture can be done by automated devices such as wearables or laboratory or other technical equipment (e.g. medical imaging, ECG equipment) ~~that are directly linked to an EDC tool~~.” |  |
| 634-636 |  | **Comment:** Clarification is required as to whether the metadata should be automatically captured by the application or manually documented.  We would suggest including the word *“relevant”* in the text below.  **Proposed change (if any):**  “Such data should be accompanied by relevant metadata identifying ~~concerning~~ the device used ~~(e.g. device version, device identifiers, firmware version, last calibration, data originator, UTC time stamp of events)~~” |  |
| 637 |  | **Comment:** This section should contain a reference to and guidance for a risk-based approach to data entry checks. |  |
| 637, 682, 693 |  | **Comment:** Consistency among sections is needed: are data entry checks intended to be performed on all data? Line 693 talks about critical data. Do we perform a double-check on all manually entered data or only on critical data identified in URS for example? Line 682 indicates the reason for change for all data changes or is it only for changes of critical data? |  |
| 638-643 |  | **Comment:** This focuses on computerized systems related to data capture but does not cover the full extent of systems mentioned by the scope set in section 2. |  |
| 645, 646 Onwards |  | **Comment:** What about informational copies? Should this be all source electronic data rather than sweeping statement of ALL data?  Generally, *“all electronic data”* is too broad a definition as it will inevitably lead to data that is not critical being audit trailed for no purpose. However, data may also be generated as part of processing e.g., approvals, which is not *“collected individual data points”* but may be critical data in that it has an impact on the outcome of the trial.  4.3 defines electronic data as *“collected individual data points”* which is appropriate for covering data collected as part of the trial. If this is the only scope, then the above requirement is probably appropriate.  Maybe there is a need for some kind of critical data definition that encompasses collected trial data and other data that can have an impact on the outcome of the trial. |  |
| 645-690 |  | **Comment:** Legacy systems are still in use and users need to establish documented means to be GCP-compliant. The current text is too prescriptive and should be adjusted to account for legacy systems where some aspects of audit trail (e.g., reason for change) may be documented to be recorded in other controlled documents, human readable audit reports can be generated by admin users. |  |
| 649 |  | **Comment:** We would propose to delete the term *“robust”* as this is not specific or quantifiable.  **Proposed change (if any):**  “Audit trails should ~~be robust~~ adhere to ALCOA ++ requirements and it should not be possible for “end ~~normal~~” users to deactivate them.” |  |
| 652 |  | **Comment:** We would propose deleting the term *"access”* from this section to avoid misinterpretation.  **Proposed change (if any):**  “Entries in the audit trail should be protected against change, deletion, and ~~access~~ modification (e.g. edit rights, visibility rights).” |  |
| 653 |  | **Comment:** The rationale for mandating that the audit trail should not be stored outside the *“system”* is unclear (where with *"system"* it is meant application; if it is meant *"system"* in a broader sense then this is a redundant statement). In some cases, it might be better to have the AT in a separate "supervisory" application. The key theme is that the AT, wherever it is located, meets the requirements for ATs (immutability, link to record, content).  **Proposed change (if any):**  Please delete the following sentence:  “~~The audit trail should not be stored outside the system.~~” |  |
| 655 |  | **Comment:** *“humanly”* does not sound correct.  **Proposed change (if any):**  “audit trails should be in a human ~~humanly~~ readable format.” |  |
| 656-658 |  | **Comment:** In preference to the export of the audit trail and the associated controls that would need to be applied in to meet confidentiality and traceability requirements for clinical data, an alternative would be to allow for the system generating the audit trail to support external tools to perform these analyses directly against the metadata.  Clarification is requested as to whether *“the entire audit trail should be available as an exported dynamic data file in order to allow for identification of systematic patterns or concerns in data across trial participants, sites etc.”* also means study level (i.e., audit trail for entire study).  More clarification is needed on the dynamic file. The definition of dynamic file formats contradicts the requirements of audit trail data. A dynamic data file can have the data changed by a user. This is not entirely what is wanted for exported AT data.  Please clarify the term dynamic, particularly in the context of AT data. |  |
| 656-660 |  | Many GCP systems do not always capture the reason for a change when a change is made and only captures the person’s name, date, previous value, new value, and relevant field identifier(s). The reason for change (why) will be a challenge also for institutions’ own systems like eMRs. Sometimes the original information is not changed but is instead supplemented.  Should this align with Good Documentation Practices?  “When” is open to interpretation. The real change happens when someone enters a character (e.g., key press on a keyboard), then the next change happens when they press the second key. We do not think key-stroke level auditing is required or useful in this context. There are other points in time when we might consider the change is "made". 1) When someone begins to edit a record (i.e., this is the point in time where it is decided to change data; it could be multiple field values on a single record); 2) When someone changes a field value on a record; 3) When someone "commits"/saves a record with one or more changes to one or more fields (i.e., this is the point in time when it is decided that the changes made are correct and should be saved (made immutable)).  All of these three options will share the same issue; a person can pause during the data entry, and then the actual audited time will never be the real change time (the only way to get the “real” time is with keystroke auditing).  We appreciate clear guidance on these approaches, or preferably a statement that all reasonable approaches have an inherent discrepancy with the real-world time that keys were pressed, and that the AT must allow for establishing accurate "relative sequencing" of events (rather than absolute universal accuracy).  **Proposed change (if any):**  “(reason for change, whenever not completely obvious)” |  |
| 661-669 |  | **Comment:** We would suggest including a section on data changes instead of addressing as part of audit trail.  **Proposed change (if any):**  Please move the following sentence from the section of audit trail to the section of data changes 5.1.1.4:  “A procedure should be in place to address the situation when a data originator (e.g. investigator or trial participant) realises that she/he has submitted incorrect data by mistake and wants to correct the recorded data. It is important that original electronic entries are visible or accessible (e.g. in the audit trail) to ensure the changes are traceable. The audit trail should record all changes made as a result of data queries or a clarification process. The clarification process for data entered should be described and documented. Changes to data should only be performed when justified. Justification should be documented. In case the data originator is the trial participant, special considerations to data clarifications might be warranted. ~~See Annex 5 section A5.1.1.41 for further details.~~” |  |
| 671-672 |  | **Comment:** *“data should not be edited or changed without the knowledge of the data originator prior to saving”* It is unclear what situation is depicted here. However, if this represents a situation where a trial subject decides to change prior entries retrospectively, this should also not be possible or limited to an agreement with the investigator. Otherwise, a risk could arise that subjects are changing their mind about entries and updates made retrospectively, and data may not truly reflect the current status of the subject/patient.  We do not think it is advisable to be monitoring the patient as they go through their thought process on the device. Once the patient commits to their answers by saving them, any changes should be tracked. To track before they save to device is intrusive and could be seen as an invasion of privacy.  **Proposed change (if any):**  “Such data should not be edited or changed without the knowledge of the data originator after saving to the device ~~prior to saving~~.” |  |
| 673 |  | **Comment:** We would propose adding an additional statement following line 673 to allow provisions when the patient does not have access to making changes to their data.  **Proposed change (if any):**  **Addition**  Please add the additional statement following line 673:  “If changes or edits to the data are required and they cannot be made by the data originator at the investigator site (including cases where the originator is the patient who does not have access to the system for change purposes), there needs to be a documented process to guide who can make the change on behalf of the site with appropriate controls in place. The changes will require an approval by the investigator.” |  |
| 676 |  | **Comment:** We cannot set the relevance of tracing the transaction time – that this is indeed short (minimised) should be possible to demonstrate as part of the technical setup ensuring ALCOA (++) principles.We would suggest at least to explain why this is relevant and to remove the term *“short”* to avoid ambiguity.  **Proposed change (if any):**  “The duration between initial capture in local memory and upload to a central server should be ~~short and traceable (i.e. transaction time)~~ minimised, especially in case of direct source data entry.”  Alternatively, please explain why traceability is relevant and remove the word *“short”*:  “The duration between initial capture in local memory and upload to a central server should be ~~short and~~ traceable (i.e. transaction date/time), especially in case of direct source data entry.” |  |
| 678-679 |  | **Comment:** Statements are contradicting. Also, what do we mean by *“extracts for internal reporting”*? |  |
| 679-680 |  | **Comment:** The rationale for audit trail entries for actions that do not change data is unclear, within the scope of GCP compliance. There may be other reasons for recording these activities in an event log (e.g., monitoring data exfiltration (security), or local privacy requirements), but these are not relevant to the audit trail in GCP contexts.  The requirement to capture the generation of data extracts and exports goes somewhat beyond existing requirements and could cause major changes and investments into existing systems. Has data extraction/export ever been in the center of a data integrity issue?  **Proposed change (if any):**  Please delete the following sentence:  “~~However, the database audit trail should capture the generation of data extracts and exports.~~” |  |
| 681 |  | **Comment:** We believe it is reasonable that we enter data to multiple fields on a single CRF page, then save them together. The rationale for not allowing this is unclear.  We would propose amending the text as follows to clarify that the audit trail should capture data changes upon saving.  **Proposed change (if any):**  “Audit trails should capture any changes made in data fields ~~in data entry per field~~ and not per page (e.g. CRF page) at the time of saving.”  Alternatively, we would suggest to change this statement to a context-based approach:  “Any changes in data entry should be automatically captured in audit trails sufficiently frequently to ensure that potentially unacceptable changes may be detected by a subsequent audit trail review. Saving must be performed ~~Audit trails should capture any changes in data entry~~ per field ~~and not per page~~, unless a documented assessment concludes that the above may be achieved by other means (e.g. by saving per CRF page)”. |  |
| 682 |  | **Comment:** “*the edit check should be part of the change rationale”* – this goes beyond existing regulations and could cause major changes and investments into existing systems.  By *“edit checks”*, do you mean double-checks of data? |  |
| 684 |  | **Comment:** The meaning of *“review”* in this sentence is unclear: *“metadata could also include (among others) review of access logs, event logs, queries etc.”*  *"Review"* is an activity, it is not (meta)data. It is not clear how metadata can include *"review of access logs"*.  This sentence is also repeated in lines 702-703, where the context seems to be more fitting.  **Proposed change (if any):**  “In addition to audit trail, metadata could also include (among others) ~~review of~~ access logs, event logs, queries etc.” |  |
| 686- 687 |  | **Comment:** More clarification and examples are needed. It would be good if metadata is defined in this context somewhere in the document so as to have a consistent interpretation. |  |
| 691 |  | **Comment:**  As per section heading, it is intended to include Audit Trail review. However, the section includes guidelines on Data review.  While the section mentions audit trail review, the paragraph is a bit confusing as it mainly relates to data review. It would be possible to interpret it as review of the clinical data in the system. We would suggest to re-phrase it accordingly.  Also, it would be great to state that data reviews and audit trail reviews should be used in a complementary way.  **Proposed change (if any):**  Section heading for 6.2.2.: “Data Review and Audit Trail Review” |  |
| 692 |  | **Comment:** The guideline states that audit trail reviews “*should generally be documented*.” What does “*generally*” mean? We would suggest deleting the word since it is vague.  **Proposed change (if any):**  “Procedures for risk-based trial specific audit trail reviews should be in place and performance of data review should ~~generally~~ be documented.” |  |
| 694 |  | **Comment:** *“unless justified”*. Please provide reasons for justification. |  |
| 696 |  | **Comment:** Processes for assessing missing data may also exist, in addition to an audit trial review. Therefore, it should be stated that processes should be implemented to help identify missing data rather than dictate the type of process that is required. |  |
| 702-703 |  | **Comment:** The examples provided in this sentence are not examples of metadata. Therefore, we would propose removing the word metadata to eliminate any potential confusion.  **Proposed change (if any):**  “In addition to audit trail review, ~~metadata~~ review could also include (among others) review of access logs, event logs, queries etc.” |  |
| 704 |  | **Comment:** *“navigate audit trail of own data”* does not sound correct.  Clarification is required as to whether sponsors should require investigators to review the audit trails in systems and document their review (and train them on how and when to do this) or if it is sufficient for sponsors to show investigators how to access and navigate the audit trails should they want/need to review them.  Please specify what level of audit trail introduction is adequate.  **Proposed change (if any):**  “The investigator should receive an introduction on how to navigate the audit trail of her/his own data in order to be able to be able to review changes.” |  |
| 706-739 |  | **Comment:** We recommend the Agency   * aligns with other agencies’ guidelines\* for a uniform approach for multicenter trials across geographies, and * accepts alternative and enduring evidence of supervision for novel technologies (e.g., electronic workflows, e-approval, etc.).   As stated by the Agency, the investigator signature is one evidence for supervision. Conceptually, the collection of a signature aligns better with CRF in paper format. Expectations on frequency become impractical in electronic format and are infeasible in some of the key evolving technologies for direct digital data capture.  **\*Other agencies guidelines:**   * ICH GCP E6R2 – 8.3.14 “SIGNED, DATED AND COMPLETED CASE REPORT FORMS (CRF)”, to document that the investigator or authorised member of the investigator’s staff confirms the observations recorded * FDA, US - Guidance for Industry on Electronic Source Data in Clinical Investigations:   *“Clinical investigator(s) to review and electronically sign the completed eCRF for each subject before the data are archived or submitted to the agency. If changes are made to the eCRF after the clinical investigator(s) has already signed, the changes should be reviewed and electronically signed by the clinical investigator(s).”*   * MHR, UK - GCP Grey Guide, section 11.5.3   *“The records should be approved by the PI or delegated member of the staff upon completion (this may be per page or per CRF dependent on the CRF template used)”*   * PMDA, Japan - Operational Guidance of Japan-Good Clinical Practice (J-GCP), Article 47   *“The investigators etc. shall prepare CRFs accurately in compliance with the protocol and shall affix the name(s) and seal, or sign the forms.”*   * NMPA, China. Technical Guidelines on Electronic Data Capture for Clinical Trials   *“After the completion of data entry and closure of all data queries, the investigator should affix electronic signature to the eCRF in the EDC system. After signature, the EDC system generally no longer permits further data changes. If any data is changed after signature, the electronic signature will be invalid.”* |  |
| 707 |  | **Comment:** We would propose removing *“and other EDC tools”* to better clarify this section. Specifically related to EDC tools, some data is reviewed although not signed off.  We recommend a consistent use of terminology (e.g., eCRF vs EDC data) in this section. While the first line in the section covers EDC tools, from line 709 until the end, eCRF data is clearly stated.  **Proposed change (if any):**  “The investigators are responsible for data entered into eCRFs ~~and other EDC tools~~ under their supervision (electronic records).” |  |
| 709 |  | **Comment:** Please replace *“attributable, legible, original, accurate, and complete and contemporaneous”* by the terms used in ICH 4.9.1.  **Proposed change (if any):**  “The signature of the principal investigator (PI) or authorised member of the investigator’s staff is considered as the documented confirmation that the data entered in the eCRF and submitted to the sponsor are ~~attributable, legible, original, accurate, and complete and contemporaneous~~ accurate, complete, legible, timely, attributable and original. (ICH-GCP 4.9.1.).” |  |
| 715 |  | **Comment:** Proposed modification for clarification.  **Proposed change (if any):**  “The acceptable timing and frequency for the sign-off needs to be defined ~~and justified for each trial~~ by the sponsor” |  |
| 716 |  | **Comment:** Clarification is required as to whether the risk-based rationale should be documented in the Data Management Plan or Study protocol design document. |  |
| 721 |  | **Comment:** *“It is essential that data are confirmed prior to interim analysis and the final analysis and that important data related to e.g. reporting of SAEs, adjudication of important events”*  It is not clear what is expected of Event Adjudication data. Is it expected that event adjudication data are signed individually the same way as we do with SAEs? |  |
| 724-726 |  | **Comment:** This paragraph is subjective, does not add to the information preceding and following, and is unnecessary.  **Proposed change (if any):**  Please remove this paragraph:  “~~Therefore, it will rarely be sufficient to just implement one signature immediately prior to database lock. Signing of batches of workbooks is also not suited to ensure high data quality and undermines the purpose of timely and thorough data review.~~” |  |
| 726 |  | **Comment:** Timely review of eCRF data can be demonstrated by data cleaning activities and site team/investigator responses to queries via audit trail, so the expected timepoint (after first entry) of investigator signature should be made clear, otherwise this may increase site burden to continually sign off data after every data query change. |  |
| 729 |  | **Comment:** One of the challenges seen at investigator sites is the timing of approval of CRF pages by the principal investigator. Clarification is required as to whether it is acceptable to have mass signing of all CRF pages at once prior to planned interim analysis or if each CRF page should be signed independently by the principal investigator. Additional guidance around timing of such signoffs is recommended. |  |
| 733 |  | **Comment:** Clarification is required as to whether evidence of principal investigator review of data is considered to be part of the audit trail review process and whether this review can be used in lieu of the sponsor or CRO doing it. More clarity regarding what constitutes the data review, that has become required over the past few years, is needed. |  |
| 745 |  | **Comment:** We would recommend deleting the first sentence or replace *“faithful”* with a definitive wording as this does not provide clear direction. Subsequent sentences are clear on the requirements for the copy so the first sentence adds no value and may potentially add more ambiguity.  **Proposed change (if any):**  Please delete the following sentence:  “~~Copies should contain a faithful representation of the data and contextual information.~~” |  |
| 755 |  | **Comment:** We would propose amending the text as follows for clarity.  **Proposed change (if any):**  “Either way the result of the copy process should be verified either automatically by a validated process or by hand to ensure to have the same ~~information, including~~ data and metadata ~~that describe the context, content and structure,~~ as the original.” |  |
| 758 |  | **Comment:** *“copies of data and metadata is provided”* – shouldn’t this be an *“are”*?  **Proposed change (if any):**  “copies of data and metadata are ~~is~~ provided” |  |
| 764 |  | **Comment:** We would propose amending the text as follows to avoid the ambiguity of use of general terms such as *“Special considerations”* and to provide more specific requirements.  **Proposed change (if any):**  "~~Special considerations should be taken~~ Certified true copies must be used whenever copies are used to replace original data ~~source documents~~" |  |
| 764-766 |  | **Comment:** The term *“GCP non-compliant”* is too strong to be used in a guidance. Please specify what clinical standard/GCP section this requirement is referring to if considered GCP non-compliant. |  |
| 767 |  | **Comment:** Please consider providing clarification in this section regarding defining which data is being discussed. Does this section refer to data during the conduct of a study or the archival of data?  This whole section should be exclusive to source data or maybe *"trial participant data"*, but not all trial data (trial data includes randomization lists, manufacturing records, etc.)  In light of the evolution in technology allowing the site to download certified copies, we recommend the Agency to address the site-related responsibilities accordingly.  **Proposed change (if any):**  Section heading for 6.6: “Hosting and control of trial participant data” |  |
| 767 |  | **Comment:** This section, as written, might cause much debate and interpretation.  *“independent third party”* could be added to the definitions’ list. It is unclear what defines an independent third party - is a platform vendor contracted by the sponsor considered independent? We need a definition and use case; one could argue that any vendor who has a financial interest with a sponsor cannot be considered independent. This term has been criticized by NCA as non-existing since the sponsor will typically pay the third party.    Regarding access and security, access will often be restricted so only the investigator can see the data, however the vendor will have IT administrators who can access upon request by the investigator. In cases where there will be a Data Processing Agreement between the vendor and the investigator, would this approach be acceptable by EMA? In case of a third party hosting data on behalf of the sponsor, the sponsor should have an oversight and established contractual agreement to ensure the data is secure, safe and compliant with relevant regulations.  Some of the data may be collected externally to clinical sites (e.g., ePRO, wearable / sensor data). The text should clarify investigator’s access to all data, not just data collected at clinical sites with consideration to data that could be unblinding.  We suggest a specific definition of “exclusive control”, because in a computer science world “exclusive control” means that there is only one party having access to a resource/data.  In context of IT systems and “exclusive control or sole control” we suggest using specific terminology to understand which technical solutions are “fit-for-purpose” or not e.g., investigators must always be able to read and write, delete and modify their data during clinical trial execution, with the sponsor in parallel being able to read that same data and if requested by the investigator, write, delete or modify data to ensure its integrity.  In a situation where the sponsor or independent third party has read, written and deleted data in parallel with the investigator, we understand the intention is not actually to do with exclusivity but about the ability of rogue actors within a sponsor to modify records without it being detectable by the sponsor, investigator and/or regulatory authorities.  Controls could be a separation of duties between the sponsor and the independent third party built on as per a technical architecture design that eliminates undetectable data tampering.  Please review, simplify and clarify this section. |  |
| 768 |  | **Comment:** There may be occasions when data collected could be regarded as “blinded” data. Therefore, the document should respect these events and provide direction for sponsors on how to deal with that.  **Proposed change (if any):**  “All data generated at the clinical trial site relating to the trial participants should be available to the investigator at all times during and after the trialunless the data will unblind the study, in which case it will be made available to the investigator once the trial is unblinded.” |  |
| 769 |  | **Comment:** Clarification is needed on exclusive control by the sponsor. There should be explicit Segregation of Duties (SoD) between sponsor’s and investigator’s access. |  |
| 770 |  | **Comment:** We would suggest clarifying that this refers to patient data.  **Proposed change (if any):**  “All patient data held by the sponsor that” |  |
| 770- 772 |  | **Comment:** Is the expectation to have a copy of the trial data?  There should be a mechanism to prove the trial data has not been tampered during the course of the trial conduct. |  |
| 773 – 779 |  | **Comment:** This paragraph is not very clear with respect to the question, whether downloading a copy of the data satisfies the requirement or if data should in any case be held at an “independent third party”.  Please re-word in an unambiguous manner. |  |
| 778 |  | **Comment:** Can this expectation be clarified to confirm that systems should have features for investigators to download a contemporaneous certified copy of the data, rather than an expectation that investigators are constantly downloading data during the course of a trial?  When a sponsor builds, provides and maintains the entire e-source/eCRF system used by patients/investigators and when hosted under the condition described in section 6.6, please clarify explicitly if the software with the functionality enabling the investigator to download their own contemporaneous certified copy from the system directly can be considered sufficient independence.  **Proposed change (if any):**  “In order to meet the requirements, the sponsor should ensure the investigator ~~should be able to~~ can independently download a contemporaneous certified copy ~~of the data~~. Any contemporaneous copy cannot have been held by the sponsor. The sponsor can via an independent third party arrange the distribution of a contemporaneous certified copy or provide software/system functionality that enables the investigator to (at their own discretion) download a contemporaneous certified copy.” |  |
| 780 |  | **Comment:** We would propose amending the text as follows since the whole legally mandated duration would already take into consideration local laws.  **Proposed change (if any):**  “Data entered into ~~to~~ EDC tools by the investigator should be available to the investigator throughout the whole legally mandated duration (for example, including ~~and for the full duration of~~ local legal requirements).” |  |
| 782 |  | **Comment:** The term *“contemporaneous local copies”* should be clearly defined. |  |
| 784 |  | **Comment:** Clarification is required as to the mechanism for future proofing the provision of a copy of the data entered in the EDC to the investigators. |  |
| 785-787 |  | **Comment:** *“In the situation where an independent third party hosting the data. the copy should not be is provided via the sponsor, as this would temporarily provide the sponsor with exclusive control over the data and thereby jeopardise the investigator’s control.”*  Although it would be ideal to use an independent third party to distribute a copy of the site data, the sponsor should have the option to perform the role to distribute the copy of data as well as long as the sponsor assures that the investigator has continuous read-only access to their data and access is not revoked until the sponsor gets confirmation from the site that they have downloaded or received the copy of the data and the copy was found to be readable by the site staff. This way the investigator will always have control over their data.  Since this is a copy, we do not believe that the sponsor would have an exclusive control over the data, which would still be controlled by the independent third party.  **Proposed change (if any):**  We would suggest further clarifying the expectations or deleting the sentence. |  |
| 786 |  | **Comment:** *“hosting the data. the copy”* a full stop has been used instead of a comma.  **Proposed change (if any):**  “hosting the data~~.~~ , the copy should not be provided” |  |
| 788 |  | **Comment:** *“advanced technical skills”* is vague and ambiguous. We require that investigators have *“advanced technical skills”* in certain areas; it is a requirement that they are medically trained for example.  Please clarify what is meant by *“advanced technical skills”*. |  |
| 788-791 |  | **Comment:** Further clarification on the expectation of *“sufficient time for the investigator to review the copy”* would be beneficial. |  |
| 792 |  | **Comment:** The rationale for the investigator to have control over hosting is unclear. It is suggested that this refers instead to access.  **Proposed change (if any):**  “Any contractual agreements regarding hosting should ensure investigator access ~~control.~~” |  |
| 798-817 |  | **Comment:** Section 6.7 on Cloud solutions – cloud solutions do not seem to be a preferred solution for the EMA. Globally, the “Cloud” does not appear to be well covered in the document. It isn’t really considered in the Annex 4 (“Security") neither. Sections 4.11 (“Direct access to computerised systems”) and 6.11 (“Database decommissioning”) can also become complex with cloud environments and agile methodologies. |  |
| 798 |  | **Comment:** Please correct the below sentence.  **Proposed change (if any):**  “Irrespective of whether a computerised system is installed at the premises of the sponsor” |  |
| 807-808  Section 6.7 |  | **Comment:** The sentence does not read properly as it is.  **Proposed change (if any):**  “In case of cloud solution being used the sponsor (ICH-GCP 5.2.1) and/or ~~of~~ the investigator (ICH-GCP 4.2.6) should ensure that the contracted party providing the cloud is qualified (see Annex 4).” |  |
| 809-810 |  | **Comment:** Is this necessary since a risk assessment needs to be undertaken by every company in the current computer environments?  The proposed wording is too subjective: we would suggest to delete the second part of the sentence.  **Proposed change (if any):**  “By using ~~buying in~~ cloud computing, the sponsor and/or investigator are at a certain risk~~, because many services are managed less visibly by the cloud provider~~.” |  |
| 811 & onwards  915-967 |  | **Comment:** Cloud solution providers such as Amazon, Microsoft, Google have been historically challenging to authenticate. Line 811 onwards discusses contractual obligations as being detailed and explicit, including data jurisdiction – more guidance is needed from the regulator as to fit for purpose/risk-based expectations.  Does Amazon, Google, Microsoft also make their cloud server hosting environments available to regulators for inspection?  Section 6.8 – Adequate back-up of data – has also been historically challenging to authenticate for cloud-based providers.  Please add more guidance. |  |
| 816 |  | **Comment:** The requirement may not be operationally feasible every time. Making a test environment available that is identical to the production environment may not be realistic.  It is not clear how one can confirm that the test environment is identical to the production. In addition, adequate qualification is already part of the security and risk assessments that a company undertakes when utilizing any computer system.  There should be a provision to verify the builds in the lower environment equivalent to the production environment with access enabled to the sponsor company. In situations wherein this is not achievable, a suitable assessment along with the mitigation should be available.  In addition, *“choses”* has been used instead of *“chooses”*.  **Proposed change (if any):**  “If the responsible party chooses ~~choses~~ to perform his own qualification of the computerized system, the cloud provider should make a test environment available which is equivalent or comparable ~~identical~~ to the production environment.” |  |
| 821 |  | **Comment:** *“at risk to be lost”* does not sound correct.  **Proposed change (if any):**  “therefore at risk ~~to be~~ of being lost.” |  |
| 850 |  | **Comment:** In situations where tools used for data migration get qualified/validated using mock data, there should not be a need to perform additional data verification post migration. It should be acceptable to rely on a qualified/validated tool to perform data migration. A risk-based approach is recommended, as suggested below.  **Proposed change (if any):**  “A data verification focused on key data, may ~~should~~ be performed post migration, depending on the outcome of a risk assessment.” |  |
| 857-858 |  | **Comment:** *“A detailed explanation is expected, why no system was available, which allowed migration of data and audit trail.”* Clarification of the meaning of the sentence is required. |  |
| 859-860 |  | **Comment:** This is true for every activity, e.g., this is a true statement if several parties are involved in Archiving (see sub-section 6.10), but the statement is missing from sub-section 6.10. It would be easier to make a single statement that any activity involving a third party requires contractual arrangements to be in place; it is not necessary to repeat this statement in multiple sections throughout the document. |  |
| 862 |  | **Comment:** It would add value to reference to EU regulation where such retention period may be found.  Please add references to EMA documentation describing retention periods for clinical trial records. |  |
| 865 |  | **Comment:** We would propose amending the text as follows for consistency with preceding sections.  **Proposed change (if any):**  “It should be clearly defined which data and documents is related to each clinical trial activity and where this record is located and who has access/edit rights to the document.” |  |
| 869 |  | **Comment:** It is not entirely clear what *“the file”* refers to. Please clarify what *“the file”* mentioned in this sentence refers to.  **Proposed change (if any):**  “It should be verified that the file remains accessible and readable depending on the media used for storage and available software through the retention period. This could imply e.g. migration of data (see section 6.9).” |  |
| 875 |  | **Comment:** The reference should be 4.11. Direct access to computerised systems (not 4.6).  **Proposed change (if any):**  “For direct access please refer to section 4.11 ~~4.6~~.” |  |
| 878 |  | **Comment:** Consideration should be given to include a realistic timeframe for the period of time that a database should be accessible. It would not be feasible in many cases to reinstate old databases when operating systems have been upgraded several times in the intervening period. |  |
| 879 |  | **Comment:** In cases where multiple trial databases are managed within one EDC system, and it is not possible to decommission individual trial databases, clarification is required as to whether there are any expectations for locking the trial database within the EDC system and making it inaccessible to users. Guidance on such situations is recommended.  Given the retention requirements for clinical data, having data maintained in a dynamic format for the entire retention period is impractical and prohibitive. Data should be maintained in such a format for as long as is practical; however, when decommissioning does occur, a documented risk assessment should be completed to determine whether the dynamic format can be maintained. Alternate formats should be allowable over time based on a robust risk assessment and provided the content, context, meaning, and metadata are maintained. |  |
| 882-883 |  | **Comment:** Please clarify this section. What is a *"certified"* copy of the database and/or how is that certified?  *“In case of decommissioning, the sponsor should ensure (contractually if done by a contracted party) that archived formats provide the possibility to restore the database(s). This includes restoring of dynamic functionality.”* It means keeping the database live for extended periods of time, and maybe even unlocking at the time of inspection. It may also mean keeping the hardware, software licenses and operating systems running, which in times of frequent technology changes is impossible to do or not even supported by the original provider. |  |
| 886-887 |  | **Comment:** We suggest the Agency to clarify the expectations around dynamic file and retention duration. |  |
| 890 |  | **Comment:** Databases decommissioning and related data archiving should be done in a static format since archiving the dynamic format of data is not suitable for long term preservation. In addition, since only the static format of data is used for submission to Health Authorities and for regulatory purposes, the rationale for archiving dynamic data is required.  **Proposed change (if any):**  “Static formats of dynamic data should ~~will not~~ be considered adequate.” |  |
| 892-927 |  | **Comment:** This section is confusing and appears to be combining requirements for contracts with vendors that provide a common service or system for use across multiple clinical trials, and a contract for a specific service or configuration of a system for a specific protocol. |  |
| 893-894 |  | **Comment:** *“in the area of”*: We would suggest to change the wording to make it clearer.  **Proposed change (if any):**  “especially including ~~in the area of~~ computerised systems” |  |
| 895 |  | **Comment:** Why limit system/services to those *“used by others”*? Guidance is missing on how to deal with truly new solutions and first use in clinical trials. |  |
| 896 |  | **Comment:** *“Accomplished”* is not clear.  **Proposed change (if any):**  “Sponsors/investigators can delegate tasks to a~~n accomplished~~ third party” |  |
| 901-972 |  | **Comment:** It would be helpful to clarify who the responsible party is, perhaps in the contract or something similar.  **Proposed change (if any):**  “The responsible party, as defined in (or defined by)…” |  |
| 904 - 905 |  | **Comment:** We would propose the below change, as this is contrary to the concept of protocol simplification.  **Proposed change (if any):**  “This should be carefully documented, in ~~the protocol,~~ procedures, contracts or agreements and other documents.” |  |
| 915-917 |  | **Comment:** Does access to vendor documents mean on-demand direct access or is period verification during vendor audits sufficient? Some Vendors do not provide some documents claiming IP or trade secret.  Certain Cloud Providers do not allow for pre-qualification audits or access for GCP inspectors; however, they could still be assessed for compliance through Public Information Assessments and review of publicly published information. We would suggest including provisions, as suggested below, for such IAAS/PAAS providers.  **Proposed change (if any):**  “If appropriate contracts cannot be put in place, e.g. because a contracted party does not allow provision of for example provided ~~e.g.~~ access to system requirements specifications, pre-qualification audits or access for GCP inspectors, or in case of cloud providers when vendor suitability cannot be confirmed through other equivalent means such as Public Information Assessments, systems from such a vendor shall not be used in clinical trials.” |  |
| 916, 986 |  | **Comment:** Please provide the definition of *“pre-qualification audit”* such as 1) audit prior to qualification activities? 2) audit with the objective to qualify a vendor/supplier? Or other 3)? Please clarify. |  |
| 918-919 |  | **Comment:** *“All parties involved in the conduct of the clinical trial should comply with ICH-GCP and this includes vendors of computerised systems.”*  It is not clear what this means specifically for CS suppliers/vendors, which are not directly GxP regulated.  This is not the case for most computer system vendors especially high-profile vendors of clinical trial systems (including both COTS and SaaS). They do not claim to need to be compliant to ICH because they do not claim to be under pharmaceutical/healthcare regulatory jurisdiction as they are only providing a system and the sponsor is accountable for its compliant use. This is often stipulated in contracts and during audits. This will represent an unprecedented change in expectations for system vendors and compromise compliance immediately upon it going into effect. |  |
| 918-923 |  | **Comment:** The GCP training for personnel at vendors and at site needs to be appropriate to the significance of the role that they play in relation to the clinical trial. For example, administrative staff who do not perform protocol specific activities do not require GCP or protocol training. |  |
| 924 |  | **Comment:** Many systems are not built specifically for each protocol anymore but rather are built to be configurable to protocol specifications.  Unless there is another meaning for protocol, the value of including such detail in the protocol is not seen.  The proposal is contrary to the concept of protocol simplification.  **Proposed change (if any):**  “The protocol, implicitly, defines part of the specification for system build or configuration” |  |
| 924-927 |  | **Comment:** This is overly specific to a single use case. This is only relevant if the software is custom made for the protocol. Otherwise, it implies that every computerised system vendor would need to review and approve the contracts for each and every trial and protocol involving their system.  **Proposed change (if any):**  “In addition, ~~it should be clear how subsequent changes to the protocol are handled so that the vendor can implement changes to the computerised system appropriately~~ vendor contracts should include provisions for handling changes to a computer system requested by the responsible party (sponsor/investigator).” |  |
| 933 |  | **Comment:** We would propose amending the text as follows to allow for the use of ancillary documentation in addition to the contract.  **Proposed change (if any):**  “It should be clear from the contract or equivalent which party is retaining and maintaining which documentation and how and in what format that documentation is made available when needed e.g. for an audit or inspection.” |  |
| 942-944 |  | **Comment:** If this is including Computer System Vendors, several prominent SaaS vendors (Oracle Veeva) while agreeing to help support inspections by providing documentation continue to contend that they are not subject to the GxP regulations and as such would not agree to be inspected by such authorities. Rather, they contend that is the accountability of the Sponsor. So, while the contract should specify the level of support the vendor will provide during regulatory inspections it is unrealistic to expect that they will agree to inspections themselves. |  |
| 943 |  | **Comment:** The guidance mentions the vendor sites, but virtual / remote audits should also be considered. |  |
| 945 |  | **Comment:** Clarification with regards to what short timelines are would be helpful. References to serious breaches might be appropriate in some instances. |  |
| 946 |  | **Comment:** We would suggest being more specific.  **Proposed change (if any):**  “To avoid undue delay in sponsor reporting from the time of confirmation of a security breach ~~discovery~~….” |  |
| 949-953 |  | **Comment:** Some is a repetition of section 8.1, so perhaps it is not necessary to repeat, but just bring clarity to expectations specifically in relation to electronic documents. |  |
| 954 |  | **Comment:** When a database is decommissioned, data may be available in an archive system and restore may not be possible because of retired software, platforms etc.  Usually, after the decommissioning of a legacy application, the data and metadata, but not the full functionalities, are archived throughout their retention time in order to give the possibility to retrieve the data in case of audit or inspection.  The requirement for restoration, especially the word *“full functionality”* should be clarified. Does it mean the full functional application or data only?  **Proposed change (if any):**  “~~Arrangements about decommissioning of the database(s) should be clear, including the possibility to restore the database(s) to full functionality (including dynamic features) for instance for inspection purposes.~~  When a database is decommissioned, the data, metadata and audit trail should be retained either in an archival system or a successor system available to review for inspection purposes.” |  |
| 964-966 |  | **Comment:** Clarification is required as to the level of training on topics of GCP that is expected i.e., a general awareness or a more in-depth understanding of GCP, in particular for vendors that are IT focused and do not conduct actual data collection or analysis type activities. |  |
| 967 |  | **Comment:** Please provide a clear reference/link to *“related Q&A documents”*. For the audience that uses such documents, there should be a location where those records are publicly available. |  |
| 977-979 |  | **Comment:** Please refer to industry standard definitions of validation (e.g., GAMP). Testing is a subset of qualification; qualification is a subset of validation; validation covers software, process, procedures, training (not just software).  It is unclear what “configuration” means (in this context) and how to validate this. More specification is needed on what the regulator is considering here (more complex configuration of workflows or the less complex configuration of list of values that populates the dropdown boxes of fields).  Expressing Validation as two potentially different and distinct exercises (i.e., core and sponsor) is misleading as the validation of the system is the totality of what is required to demonstrate fitness for purpose and is the sole accountability of the sponsor. If the sponsor chooses to leverage activities and documentation by the vendor (after appropriate assessment) then the sponsor’s overall validation should account for that and the validation (singular) would be the combination of what the vendor contributed and what the sponsor contributed (not two separate validations). The sponsor’s validation documentation (e.g., validation plan) should define what is being leveraged and why and what is being conducted in house to demonstrate the control of the system. If for whatever reason the vendor activities/documentation cannot be leveraged, this does not preclude the use of the system by the vendor but rather, may require the sponsor to do more on their own.  **Proposed change (if any):**  “Validation should include activities and documentation for qualification/testing ~~validation~~ of the core software by the vendor for a commercial off the shelf (COTS) and/or software as a service (SaaS) ***,*** if leveraged, or activities and documentation forqualification/testing ~~validation of the software developed~~ required by the sponsor or investigator (e.g., due to additional softwareincluding ~~the use of~~ open source, unique use cases, subsequent configurations, etc.) ~~and of its subsequent configuration~~. ~~A~~ Further validation activities may be required to confirm the intended usage in terms of supporting business processes where the installed software is then used for specific trials requiring a configuration or build based on the requirements of a specific trial.” |  |
| 979-981 |  | **Comment:** Clarification is required as to the meaning of *“further validation”* in this context e.g., study UAT?  There is no mention of PQ/ UAT.  **Proposed change (if any):**  **Addition**  Please add a statement on sponsor to perform the PQ/ UAT to verify the business processes for which the computerized system is procured. |  |
| 984-986 |  | **Comment:** The sponsor may rely on qualification documentation provided by the vendor provided if the qualification activities and subsequent documentation have been assessed as adequate. Both need to be adequate (activities & documentation) in order to be leveraged.  **Proposed change (if any):**  “They may rely on qualification documentation provided by the vendor if both the qualification activities performed by the vendor and associated documentation have been assessed as adequate, but may also have to perform additional qualification/validation activities based on a documented risk-assessment e.g. during pre-qualification audits.” |  |
| 991-992 |  | **Comment:** It is inconsistent with the rest of the document and industry’s understanding to indicate that the system may be validated by the supplier but installed at the sponsor/institution as SaaS. The rest of the document discusses leveraging vendor qualification activities and documentation which is in better alignment with the expectation that the user of the system is responsible for the validation for their intended use. |  |
| 993 |  | **Comment:** We would propose amending the text to avoid the use of terms such as *“of thorough knowledge”* which may result in subjectivity.  Too much emphasis is placed on audits and increasing the depth of audits. Detailed knowledge of the vendor's system documentation for the individuals ultimately accountable cannot be gained from a single audit regardless of the depth. The depth of audit required would require increased time and auditor numbers that would likely be overly onerous and disruptive to the vendors as all sponsors increase their audit depth. Required knowledge of such systems and documentation by the accountable individuals would require an ongoing relationship with the vendor. Audits are a snapshot in time and should realistically form an integral part of an ongoing assessment by the responsible party during an ongoing working, contracted relationship with the vendor. This section should be revised to reflect audits as only part of the assessment by the responsible party required to ensure continued validation of the system and sufficient knowledge of the vendor leveraged documentation and processes to support the system during inspections.  The responsible party, or where applicable the CRO performing these activities for them, should have a detailed knowledge about the qualification documentation and should be able to navigate through it and explain the activities as if they had performed the activities themselves.  The requirement in this sentence seems to be very difficult to implement as sponsors are not the owners of the supplier validation dossier.  **Proposed change (if any):**  “For the responsible party to use the vendor's qualification documentation, they should ~~have a thorough knowledge about~~ assess the vendor's quality system and qualification activities, which could usually be obtained through an in-depth assessment/audit.” |  |
| 1000 |  | **Comment:** Please correct the sentence as proposed below.  **Proposed change (if any):**  “responsible party – e.g. by those ~~them~~ performing part of the qualification.” |  |
| 1000-1003 |  | **Comment:** Vendors do not typically provide this documentation outside of an audit and therefore we would recommend including them as a potential responsible party.  **Proposed change (if any):**  “The responsible partyincluding the vendor, or where applicable the contract research organisation (CRO) performing these activities for them, should have a detailed knowledge about the qualification documentation and should be able to navigate through it and explain the activities as if they had performed the activities themselves. Where the responsible party relies on vendors or CROs to explain the activities during inspections, this should be part of the supplier arrangements governed by agreements.” |  |
| 1009 |  | **Comment:** *“vendor’s validation environment”* This presumes a specific engagement model and validation landscape that may not be common. It is typical that the responsible party has development, qualification and production environments. Any software updates made available from a vendor will be deployed through these environments in sequence and assessed/qualified/validated as appropriate. The vendor's environment configurations may or may not be known - this depends on the engagement model and contract. What is important is building the environment to the required specification, maintaining a known build via configuration management, and establishing equivalence between environments, with known differences reviewed and assessed for risk to the validation status of the final system.  **Proposed change (if any):**  “any differences between the ~~vendor's~~ validation environment and the ~~responsible party’s~~ production environment” |  |
| 1010 |  | **Comment:** The responsible party should not just “justify” the vendor and sponsor environment differences as insignificant but should adequately assess whether or not the differences are insignificant and if so justify and document the justification. |  |
| 1011-1012 |  | **Comment:** This sentence can be misinterpreted to be any environment, including development environment, where only *“trained developers”* can have access.  We recommend providing IQ/PQ as examples rather than expectations on how to perform system validation since a risk-based approach to validation depends on the system complexity and type of technology.  IQ/PQ: these terms are not defined, and later the term UAT is used (PQ is generally understood to be synonymous with UAT, but we are not sure if this document presents the same view).  Does this imply that for fully automated systems, no IQ/PQ is required? Or if the users are not trained, no IQ/PQ is required? It seems a bit odd.  We would suggest rephrasing the sentence to be more focused on what is intended.  We would recommendation to refer to industry standards (i.e., GAMP) for definitions of CSV terms, or define the terms in this document. |  |
| 1013-1015 |  | **Comment:** The focus is only on eDC/eCRF interface. A more general wording would be more adequate.  **Proposed change (if any):**  “Interfaces between systems and tools used for clinical trial data capture ~~the electronic case report form (eCRF) and other systems~~ should be clearly defined and validated e.g. import of item response theory data, automatically generated emails to safety mailboxes etc.” |  |
| 1020 |  | **Comment:** A question mark has been added to the end.  **Proposed change (if any):**  “(EMA/INS/GCP/856758/2018)~~?~~)” |  |
| 1022 |  | **Comment:** In the requirements section, there is no mention of applicable legal/regulatory requirements to be included as part of the User Requirements process.  We would suggest mentioning the inclusion of applicable legal/regulatory requirements. |  |
| 1023-1026 |  | **Comment:** *“Independently on whether a system […]”* It is unclear if this is referring only to systems that require validation or to all systems.  **Proposed change (if any):**  “For to-be validated systems, independently of ~~on~~ whether a system is developed on request by the sponsor/institution,…” |  |
| 1025 |  | **Comment:** With CSA being lined up, this statement may need an update. Secondly, URS is meant to document the business requirements and not the functional requirements. With CSA, the expectation should be every computerized system irrespective of their development methodology and technology used should be supported by requirements specifications which is verifiable by corresponding test specifications. |  |
| 1027 |  | **Comment:** *“purchase customisation and configuration”* does not make sense. Please also correct the grammatical errors.  **Proposed change (if any):**  “The URS should form the basis for system design~~, purchase~~ (customisation and configuration), ~~but~~ and also for system qualification~~)~~.” |  |
| 1030-1032 |  | **Comment:** The requirement for referencing protocol version within specification document should also apply when changes are made to specification documents due to protocol amendments. It is recommended that any changes to trial-specific build due to protocol amendments be clearly identified in the specification documents.  **Proposed change (if any):**  “This should make reference to the clinical trial protocol and version for which it was designed, including any clinical trial protocol amendments.” |  |
| 1031-1032 |  | **Comment:** The software development additional documents for functional and design specifications are produced.  The wording and intended meaning is not clear.  Please re-word to convey original intent. |  |
| 1036-1037 |  | **Comment:** *“The sponsor/investigator should take responsibility for the URS. This document should always be reviewed and approved by the sponsor/investigator.”* This task could also be performed by a CRO or any vendor with adequate oversight. It should not necessarily be the sponsor.  Sponsors and investigators do not have exactly the same role. We would suggest removing the term investigator. We would also suggest giving the opportunity to sponsors to appoint someone to review or approve the URS.  If this is intended to include both requirements fulfilled by the vendor and by the sponsor, then this should be specified within the document. Please clarify whether it would be acceptable to have the URS represented by both the vendor documentation and the sponsor documentation. It seems in either case the expectation is that the responsible party approves the URS even if it is the vendor’s URS.  **Proposed change (if any):**  “The sponsor~~/investigator~~ or representativeshould take responsibility for the URS. This document should ~~always~~ be reviewed and approved by the sponsor~~/investigator~~ or representative.” |  |
| 1040 |  | **Comment:** The vendor’s system requirement specification may not be available to the responsible party.  **Proposed change (if any):**  “system on the basis of their own and of the vendor’s system requirement specifications, where available.” |  |
| 1044-1045 |  | **Comment:** This seems to contradict the previous statement regarding responsibility for the validation of documents. |  |
| 1051 |  | **Comment:** We contend that Requirements Traceability is the principal requirement, not the matrix itself. The traceability matrix as a document is only one mechanism for demonstrating traceability.  The requirements traceability matrix should be created irrespective of the number of requirements of any system. Current verbiage is referring to large number of complex requirements, which might create confusion to maintain TM for only a large number of requirements.  This section is written in a way which requests for document format of Requirements Trace Matrix. However, the key focus should be on identifying a process to ensure traceability which can be documented at any given point in time and be presentable to investigators/ inspectors.  We would suggest to remove the reference to the number of requirements. |  |
| 1052 |  | **Comment:** Some requirements could be met procedurally and hence may not have a test case. Clarity is needed that a requirement can be met either technically which will have a test case, or procedurally which will have an SOP reference in the Traceability Matrix.  Not every requirement will have a test case associated with it. A risk-based approach is frequently applied to determine the depth of the testing.  Every requirement should have at least one corresponding test case or have a documented rationale for how it is being met procedurally. We would suggest clarifying that a requirement may be mapped to a procedure and not necessarily a test case.  As specification documents should be maintained and updated throughout the system lifecycle as requirements to the system change, to ensure that the corresponding specification and requirement are considered as part of the change impact assessment, each specification should be traceable to its related requirement(s).  **Proposed change (if any):**  “For complex systems with a large number of requirements, it is not feasible to keep track of requirements and their corresponding test cases without having a systematic approach of documenting this, e.g. traceability matrix. This information ~~document~~ may have many forms and the process may even be automated by software, but it should be created during system development and qualification and be continuously updated as requirements are changed to ensure that for every applicable requirement (e.g., based on risk assessment), there is at least one corresponding test case. As specification documents should be maintained and updated throughout the system lifecycle as requirements to the system change, to ensure that the corresponding specification and requirement are considered as part of the change impact assessment, each specification should be traceable to its related requirement(s). The specifications should also be part of the traceability matrix.” |  |
| 1058-1073 |  | **Comment:** The validation planning and activities should be elaborated and explained further to include risk-based approaches for validation. This section has more details of testing, and much less details of validation.  It does not describe a risk-based approach to testing (e.g., non-GxP requirements could be tested by exploratory testing, rather than fully scripted). Please address the concept of risk as it relates to testing (e.g., test case format, level of evidence required, etc.) as part of the validation/qualification of systems within this section.  Moreover, no mention of functional/configuration testing (OQ) is made in this section. Any custom/configurable functionality needs to be tested as part of the OQ phase.  We would suggest to elaborate on validation planning and activities with risk-based approaches.  This section covers *“A2.4 Validation plans and test plans/scripts/case”* and not the test execution. All information related to test execution should be moved to the next section (A2.5 Test execution and reporting). In addition, evidence may have many formats (not only a screenshot as mentioned in line 1069).  This section appears to only address test plans and not validation plans. We would recommend that this section addresses the expectations of the validation plan, particularly when the validation is a combination of the vendor and sponsor activities (e.g., identifies what is being leveraged from the vendor and why, division of responsibilities, risk-based approach to testing, types of testing (low risk unscripted testing, automated testing, etc.)).  We would suggest allowing not to document the actual result as seen in the test step as long as the provided evidence gives enough details to satisfy the test step expectation and that an independent reviewer could easily confirm the expected result. Additionally, it should be allowed not to provide actual results when the expected result is simple.  **Proposed change (if any):**  “Validation activities should be planned and documented, for example validation plan and test plan. Test cases and individual test steps should be ~~pre-~~approved prior test execution ~~and conducted accordingly~~. This is required for validation of both core software and trial specific configurations/builds.  […]  Test cases should include exact reference to requirement identity, ~~version of the software being tested (target),~~ any pre-requisites or conditions prior to conducting the test, description of the step taken to test the functionality (input), expected result (acceptance criteria), and require the user to document the actual result as seen in the test step, evidence, if relevant (e.g., screen shot), conclusion of the test step (pass/fail)~~, and deviation impact assessment and subsequent decisions regarding the deviations (if applicable)~~.  In the situation whereby evidence provided gives enough details to satisfy the expected result (acceptance criteria) for an independent reviewer to identify or if the expected result requires a single and direct outcome to confirm, the user would not be required to document the actual result, but only refer to the evidence.  Test cases for trial specific configurations/builds should ensure that the system meets the specification ~~documentation~~ and therefore the clinical trial protocol requirements.” |  |
| 1074-1091 |  | **Comment:** The section on testing only considers testing performed by human operators. It is suggested that the possibility of automated testing be addressed.  Clarification is required as to whether UAT referenced here means study build UAT or UAT performed by the software developer. In addition, the Agency should clarify the responsibility for executing the UAT and what it is testing (the overall functionality or that specific to the protocol requirements).  Please amending section A2.5 to reflect changes proposed to section A2.4.  Please add more details on risk-based testing, formal and informal test executions, etc.  **Proposed change (if any):**  “Test execution should follow ~~pre-~~approved protocols and test cases (see A2.4),the version of the software being tested (target) should be documented and where applicable and required by test cases and test procedures, evidence (e.g., screen shots) should be captured to document test steps and results when relevant. The person performing each test and his access rights (role) should be documented. Where previously ~~passed~~ failed scripts are not retested along with the testing of fixes for previous fails, this should be risk assessed and the rationale documented.  Testing of the software or trial specific configurations would typically comprise ~~difference~~ different components. […]  Deviations encountered during system testing ~~qualification~~ should be recorded and brought to closure. Any failure to meet requirements pre-defined to be critical should be solved prior to deployment or deployment should be justified and potential impact thoroughly assessed. All open deviations and any known issues with the system on releaseshould be assessed and subsequent decisions regarding the impact should be documented in a validation report and, where used, release notes.” |  |
| 1075-1077 |  | **Comment:** This section does not include or support the use of electronic systems for the testing of system requirements where there is different yet fully sufficient evidence in a form other than what is traditional in a paper-based system. The use of and the results from validated testing tools is very much integrated into the industry and expanding. |  |
| 1093-1098 |  | **Comment:** *“Trial specific configurations/builds should only be released into production and made available to trained site users when all the necessary approvals**for the clinical trial have been received, e.g. regulatory authority approval and all documentation is in place (e.g. signed protocol, signed agreement with investigator). This includes any updates to the system, e.g., changes to the system resulting from a protocol amendment should only be released into production once it is confirmed that the necessary approvals have been obtained.”* Which approvals are meant (regulatory authority, IRB, EC,…)? Waiting for *all* approvals prior to production release of a tool might not be feasible in practice (e.g., delayed responses from local authorities).  In cases where approvals are required from multiple IRBs/Health agencies, it is not feasible or sometimes technically possible to release database changes into production for only those markets/countries from where approval has been obtained. In such situations, clarification is requested as to whether it is expected to wait for all approvals from all Health Agencies before changes could be released into production. In such situations, critical changes that could potentially impact patient safety could be delayed if sponsors have to wait for protocol amendment approvals from all health agencies. Such situations should allow for exceptions in terms of deploying database changes into production.  **Proposed change (if any):**  “This includes any updates to the system, e.g., changes to the system resulting from a protocol amendment should only be released into production once it is confirmed that the necessary approvals have been obtained, unless such changes mitigate urgent safety risks for the patients and/or safe conduct of the trial.” |  |
| 1104-1105 |  | **Comment:** At the end of testing and prior to release to production a validation report should be prepared and approved.  **Proposed change (if any):**  “At the end of testing and prior to release to production a formal release authorization or validation report should be prepared and approved.” |  |
| 1105 |  | **Comment:** If use procedures are expected then this should be specified here.  The term *“other resources”* should be either clarified or examples provided.  **Proposed change (if any):**  “At the time of release training materials, use procedures, and other resources for users should be available.” |  |
| 1107-1108 |  | **Comment:** The example given is *"yearly or related to major updates"*. It should be instead indicated to assess the periodicity based on the criticality of the system or on the duration of the study (e.g., if the study is only two years-long, it does not make sense to wait for three years).  **Proposed change (if any):**  “Periodic (e.g. yearly or related to major updates, and always determined on the study duration and the system risk) system reviews should be conducted to assess…” |  |
| 1114 |  | **Comment:** Section A2.7 – Please provide clarification for distinction between application changes compared to  hardware/infrastructure changes; and changes to operating system/platform. Please add some examples to illustrate this. |  |
| 1121 |  | **Comment:** While it is agreed that failed login attempts should be monitored, it is unclear why including it in the periodic review would be valuable as such attempts should be monitored in real time rather than potentially a year+ after the occurrence.  Clarification is needed on this failed login attempts, it seems out of place here. Perhaps this was meant as an indication of potential security incidents, but it is not really meaningful to know how many times someone mistyped their password.  Please clarify how failed login attempts influence the validated state of the system.  **Proposed change (if any):**  We would suggest removing the following:  “~~and failed login attempts.~~” |  |
| 1122 |  | **Comment:** Section A2.8 - Is this section referring to a real Change Control Process as in formally documented in quality management system or a change management process? Please clarify. |  |
| 1123-1129 |  | **Comment:** Lines from 1123 to 1125 provide the "minimum", whereas from lines 1126 to 1129 it provides further what the change request should include: documentation to be updated as appropriate.  We would suggest *"as a minimum"* to be removed.  **Proposed change (if any):**  “There should be a formal change control process. Requests for change should be documented and should include details of change, risk-assessment (e.g. for data integrity, regulatory compliance) and testing requirements ~~as a minimum~~.” |  |
| 1124 |  | **Comment:** Please include the impact on the validated state of the system as part of the example. |  |
| 1128 |  | **Comment:** A *“report of validation activities”* in the context of change management may not be a complete / formal report depending on the scope and complexity of the change.  A complete Change Record (e.g., in an ITSM system) including risk-assessment, list of updated deliverables, etc. should be sufficient to demonstrate the required control. |  |
| 1131-1133 |  | **Comment:** The word *“highlighted”* seems to imply a functionality in the technology hosting the change.  Protocol changes can impact a variety of systems, it is unlikely that all tools will have the same ability to highlight a change. We recommend the Agency considers communication and/or other documents as good alternatives to change visibility. |  |
| 1140 |  | **Comment:** Data can be collected by a variety of electronic means; the text in the document overall should be consistent with the example for the scope of technology covered.  This paragraph seems out of place here. We are not sure if there was an intent to connect this to formal change management or just as aspects to consider that may require a formal change management process. Please clarify the purpose of this paragraph.  **Proposed change (if any):**  “The eCRF and/or electronic data capture ~~collection~~ (EDC, ePRO) system can change during ~~the course of~~ the trial.” |  |
| 1142 |  | **Comment:** We would propose deleting the reference to audit trail system for clarification.  System changes to eCRF and/or EDC during the course of a trial are documented through change control. Current practice and system configuration is that such changes are not documented in the audit trail (which typically captures data and user account related changes). The requirement stated here that such changes should be documented as part of the audit trail system would require major system updates. Also, it is not clear why such changes should be documented in the audit trail system if the changes are documented by change control. We would propose to drop the requirement to capture system changes in the audit trail system or to specify what exact kind of changes are meant here.  **Proposed change (if any):**  “Any such changes could influence contextual properties that may change data entry behaviour, data interpretation and create issues for statistical analysis and should be sufficiently documented ~~as part of the audit trail system~~.” |  |
| 1145 |  | **Comment:** It is suggested that this annex includes a section describing ongoing periodic review of active users for the system. |  |
| 1148 |  | **Comment:** Please delete the dash added between *“the”* and *“management”*.  **Proposed change (if any):**  “end their involvement/responsibility in the~~-~~management and/or conduct of the clinical trial projects.” |  |
| 1152-1154 |  | **Comment:** Please consider defining the need of assessing the *"Suitable intervals"* as part of the validation.  **Proposed change (if any):**  “This information concerning actual users and their privileges on systems should be verified at suitable intervals to ensure that only necessary and approved users have access and that their roles and permissions are appropriate. The suitable interval should be determined together with the computerised system periodic review interval assessment.” |  |
| 1164-1166 |  | **Comment:** The guideline **s**hould also indicate that the number of administrative users should be kept to a minimum number required to fulfil the role. |  |
| 1171 – 1173 |  | **Comment:** Further definition on the scope of applicability is required e.g., sponsor, investigator, inspector. |  |
| 1175 |  | **Comment:** *“Sharing of accounts is considered unacceptable.”* This needs to be reconsidered because it is not possible to comply with this as stated. Certain system/technical accounts (as referenced in the next section as *"machine accounts"*) that are not intended for use by end users will exist. In fact, many systems require the use of a system account (e.g., root, admin) to install/build the system/services. These are controlled by the system administration team and therefore are (by design) shared across the support team. The requirements for these types of necessary shared accounts should be explained, e.g., the accounts must be tightly controlled by a privileged account management system that can ensure that use of the account is traceable to an individual.  For some technology e.g., wearable, having classic individual accounts might be challenging. We would suggest clarifying that individual accounts should apply only to a shared system.  Please revise this section to allow the use of shared accounts for specific purposes, with appropriate controls.  **Proposed change (if any):**  “All ~~system~~ usersof a shared system should have individual accounts. Sharing of accounts (group accounts) is considered unacceptable and a violation of data integrity and ICH-GCP principles as data should be attributable.” |  |
| 1178 |  | **Comment:** *“across full life cycle”* is not correct.  **Proposed change (if any):**  “within the system and across the full life cycle of the system.” |  |
| 1179 |  | **Comment:** This is perhaps too prescriptive. Instead, the guideline could just state that user accounts for interactive use should be distinguishable from machine accounts. How this happens can depend on the system itself. (For example, via an account type field).  Please clarify the definition of machine accounts.  **Proposed change (if any):**  “User accounts ~~names~~ should be traceable to a named owner and accounts intended for interactive use ~~and those assigned to human users~~ should be ~~readily~~ distinguishable from machine accounts.” |  |
| Annex 4 |  | **Comment:** In a Bring Your Own Device (BYOD, e.g., mobile phone) set-up enforcing OS update, anti-virus usage, internal activity monitoring, etc., might not be possible and illegal.  Please revise accordingly. |  |
| 1182 |  | **Comment:** Including scope is not appropriate for the title. Please consider the scope of the section for A4.1 Ongoing security measures. |  |
| 1189-1190 |  | **Comment:** More clarity is needed on how this can apply to mobile devices, e.g., mobile phones that may be used for data collection. We cannot prevent someone from losing their phone.  Please clarify the scope of this statement, and if it applies to mobile devices, please add guidance on ways to meet this requirement for those use cases. |  |
| 1191-1193 |  | **Comment:** The second sentence is not clear. Please consider rewriting to provide more clarity. |  |
| 1194 |  | **Comment:** Please clarify who is the responsible party here. |  |
| 1197 |  | **Comment:** What is meant by two factor authentication in this situation i.e., the physical access to a data centre? |  |
| 1200-1201 |  | **Comment:** This sentence is unclear – is it meant that disposable media should be properly erased before being appropriately disposed of?  In addition, can it please be clarified what *“redundant IP providers”* means? |  |
| 1201 |  | **Comment:** *“properly destructed”* is not correct.  In addition, this should include the possibility of Cryptographic Erase (CE) as described in NIST 800-88.  **Proposed change (if any):**  “properly destroyed ~~destructed~~ before being disposed of” |  |
| 1202 |  | **Comment:** *“the servers should be locked up in cages to prevent access from other clients”*: This practice only makes sense if clients have physical access to the data centers.  **Proposed change (if any):**  “Disposed media (e.g. hard disks) should be properly destructed before being disposed of and in case of co-location (see Cloud services) where clients have physical access to the data center, the servers should be locked up (e.g., in cages) to prevent access from other clients.” |  |
| 1203-1205 |  | **Comment:** The sentence implies that any system should have fail-over capability. This should, however, be based on availability requirements. If longer downtime is tolerable, a backup stored at another facility may be adequate, instead of replication. This sentence should be more reflective of a risk-based approach. |  |
| 1206-1214 |  | **Comment:** The term *“firewall”* excludes other/newer technologies which perform the same perimeter segregation control activity (such as GSDN). A common term could be “Network Policy Enforcement device”. |  |
| 1213 |  | **Comment:** It is suggested that the term *“periodically”* be defined e.g., yearly, bi-yearly, etc. |  |
| 1221-1222 |  | **Comment:** Clarification of the meaning of the sentence is required.  It is not clear how this can apply to mobile devices.  Please clarify the scope of this statement, and if it applies to mobile devices, please add guidance on ways to meet this requirement for those use cases. |  |
| 1226 |  | **Comment:** Supported systems are not automatically invulnerable, the same way unsupported systems are not completely vulnerable; it is about impact and probability (and risk).  Please consider clarifying the language.  **Proposed change (if any):**  “for which no security patches are provided ~~made~~, expose a higher risk to vulnerability ~~are in a vulnerable state~~.” |  |
| 1237 |  | **Comment:** Clarification is required regarding how to define *“controlled”* use of bi-directional devices. |  |
| 1243 |  | **Comment:** *“antivirus”* is missing a dash.  **Proposed change (if any):**  “the installation of anti-virus” |  |
| 1245 |  | **Comment**: *“anti-viral”* should be *“anti-virus”.*  **Proposed change (if any):**  “Part of using anti-virus ~~viral~~ software” |  |
| 1245 |  | **Comment:** *“Part of using anti-viral software is the need to monitor and review the task manager processes to be alerted in case the anti-virus process is terminated.”*  This isan unclear statement as to what is expected to be achieved. It would be beneficial if the “why and what” are described. This statement seems to relate to a (too) specific technological platform.  It is important to ensure the anti-virus process is not terminated but reviewing the task manager process is not the right approach. For example, McAfee has a separate process strictly protecting its registry keys, drivers and dlls and to log and create alerts whenever any other process is trying to interfere with the McAfee components in any way.  Hence, the method for how to ensure undue termination of the anti-virus process should be described in a more generic manner. |  |
| 1248-1252 |  | **Comment:** Some guidance is recommended to be included for sponsors in terms of what could be considered acceptable as evidence of penetration testing. Most of these results are confidential in nature and sponsors or cloud providers should not be expected to share such results with the inspectors. Certificates demonstrating that such tests are being performed should be deemed adequate for evidence purposes.    **Proposed change (if any):**  “Vulnerabilities identified, especially those related to a potential loss of data integrity, should be addressed and mitigated in a timely manner. Certificates demonstrating that such tests are being performed are considered to be adequate evidence of penetration testing.” |  |
| 1253-1254 |  | **Comment:** *“If the security measure requires input data modifications, reversibility and traceability should be considered as some inputs require full traceability (e.g. source data).”*: It is not clear what the added requirement is here. |  |
| 1255 |  | **Comment:** IDS is a reactive process (i.e., intrusion has happened). Intrusion Prevention systems can also be applied, with a risk-based approach, which are better as being proactive.  Please include Intrusion Prevention Systems. |  |
| 1259-1261 |  | **Comment:** This is a requirement which is very difficult to implement in reality and it may result in many false positives.  In addition, the examples provided (excessive file downloads, copying or moving or backend data changes) are not representative of insider threat.  **Proposed change:**  “An effective system for detecting ~~any unusual~~ activity assessed as unusual or risky from a user (e.g., ~~excessive~~ unusual file downloads~~, copying or moving~~ or backend data changes) should be in place.” |  |
| 1274 |  | **Comment:** The term *“Remote authentication”* appears twice in this header. This seems to be a copy/paste error.  **Proposed change (if any):**  Section heading for A4.13: “Remote authentication and password managers ~~Remote Authentication~~” |  |
| 1274-1292 |  | **Comment:** The entire paragraph is confusing because it mixes several topics (remote access, 2FA, password managers). It should be worded more clearly.  Guidance specifically on password managers is not clear. What is the expectation? |  |
| 1284-1287 |  | **Comment:** Please consider to rephrase: describe the ‘why and what'; keep to the level requirements, expectations, obligations; the statement might be too specifically targeting password managers, but this certainly is only one example to be considered. There are many more unsecure password management approaches in place, which should not be excluded from risk assessments.  Please consider providing an example where a password manager is appropriate.  Please consider robust password managers, which would not lead to any enhanced risk. |  |
| 1293-1296 |  | **Comment:** *“The policies should include but not necessarily be limited to length, complexity, expiry, login attempts, and logout reset.”*  NIST (800-63) and other organizations do not recommend composition/complexity rules or expiry time, hence the requirement here should not be strict but allow for a risk-based approach. |  |
| 1299 |  | **Comment:** This section implies that after a password is received from a manager or *“system admin”* a new password should be set by the user. This should be mandated by the system each time and not a result of a *“special occasion”*.  **Proposed change (if any):**  “This implies that after a password is received from a manager or “system admin” ~~(e.g. after a vacation)~~, a new password should be set by the user.” |  |
| 1302 |  | **Comment:** Please consider adding “locks out”.  In addition, systems used within GCP have different usage patterns and some areas will instead need to implement compensating controls. We suggest clarifying which areas within GCP should comply with this requirement.  **Proposed change (if any):**  “Systems should include an automatic inactivity logout, which logs out or lock out a user after a risk-based, defined period of inactivity.” |  |
| 1307 |  | **Comment:** We would propose replacing *“procedures”* with *“controls”* to allow either a procedural or a technical control to be in place for ensuring consistency in time.  **Proposed change (if any):**  “Where the system captures date, time and time zone and/or the date, time and time zone are required for reconstructions of activities, ~~procedures~~ controls should be in place to ensure to be consistent irrespective of location and not to be subject to amendment by users (e.g. universal time coordinated (UTC)).” |  |
| 1313-1314 |  | **Comment:** More options should be considered here as some sponsors may be customers of VPN alternatives such as ZTNA (Zero-Trust Network Access) and not be decisively included in the two options. |  |
| 1314 |  | **Comment:** *“(https))”* has an extra bracket.  **Proposed change (if any):**  “hypertext transfer protocol secure (https)~~)~~” |  |  |  |
| 1321 |  | **Comment:** A word is missing.  **Proposed change (if any):**  “because the type of data collection method is relatively new.” |  |  |  |
| 1328 |  | **Comment:** *“Data entered”* should be more specific. *"submitted"* or *"saved"* may be a better choice to clearly differentiate from when entering data into an online form.  **Proposed change (if any):**  “Data saved ~~entered~~ into the EDC tools” |  |  |  |
| 1336-1337 |  | **Comment:** It is unclear what the Agency expects with the term *“one to one correspondence”*.  We recommend that the text is aligned with the MHRA GXP Data Integrity Guidance and Definitions section 6.12 on computerised systems transactions.  **Proposed change (if any):**  “However, source data directly entered into an eCRF should be saved contemporaneously, the combination of multiple entries into a combined single transaction should be avoided, and the time intervals before saving of data should be minimised ~~in a one to one correspondence~~.” |  |  | It is unclear what the Agency expects with the term “one to one correspondence”.  We recommend that the text is aligned with the MHRA ‘GXP’ Data Integrity Guidance and Definitions section 6.12 on computerised systems transactions. Proposed text is “However, source data directly entered into an eCRF should be saved contemporaneously, the combination of multiple entries into a combined single transaction should be avoided, and the time intervals before saving of data should be minimised” |
| 1339 |  | **Comment:** There is an inconsistent use of terminologies in section A5.1. The intent of this section is to describe electronic clinical outcome assessments (eCOA) but in the subsequent sections, the content switches to other EDC tools.  We recommend using consistent terminology in this section. |  |
| 1343-1344 |  | **Comment:** The term *“eCOA tool”* is not defined. We would suggest using Digital Health Technology tool as a more generic term that can collect eCOA data.  **Proposed change (if any):**  “The guideline aims at addressing the topics specifically related to these ~~eCOA~~ Digital Health Technology (DHT) tools ~~being electronic~~ which collect COA data and also to those related to the situation where Bring-your-own-device (BYOD) solutions are used.” |  |
| 1346 |  | **Comment:** *“PIs”* is mentioned whereas *“investigators”* is used elsewhere and throughout the document.  **Proposed change (if any):**  “made available to involved/responsible parties such as the investigators ~~PIs~~ e.g. via portals, display of source data on the server” |  |
| 1347 |  | **Comment:** We suggest allowing for a more flexible approach, not only accepting processes to be described in the protocol.  We would propose amending the text as follows to allow for the use of ancillary documentation in addition to the protocol.  **Proposed change (if any):**  “These processes (including access controls) should be controlled and clearly described in the protocol or equivalent, and all parts of the processes should be validated.”  Alternatively, if EMA still requires the documentation to be available to all readers of the protocol, it will still be beneficial, if it does not have to be part of the protocol as such:  “These processes (including access controls) should be controlled and clearly described or referenced in the protocol, and all parts of the processes should be validated.” |  |
| 1354-1459  Sections A5.1.1 & A5.1.2 & A5.1.3 |  | **Comment:** We would suggest to combine these sections and refer to eCOA given that the guidance often states similar requirements across sections and COA types. We would suggest to call out where requirements differ for ePRO vs other, as needed.  Furthermore, we would suggest adding a sub-section for Performance Outcome Assessments collected by wearables/sensors, in case there are specific requirements for those, to complement the existing sections, as it is a developing field and their use in clinical trials will increase in the future. |  |
| 1356 |  | **Comment:** The recommendation to involve site staff, trial participants/patients in the development is appropriate when the intent is to evaluate the validity of the instrument itself (e.g., deploy a new device or scale for a broad use). However, it is important to consider when the data entry screens are recreating validated scales and questionnaires (public or copyrighted) or use rulers or lines that cannot be modified for usability preference of the end-users.  We would propose amending the text as follows to avoid overburdening the site staff.  **Proposed change (if any):**  “The ePRO should be designed considering copyrights, validation of translations, medical conditions for intended use and population to meet the specific needs of the protocol and of ~~the~~ end users. ~~It is recommended to involve~~ Whenever applicable, without exposing to risks the copyright and validity for the ePRO tool, site staff or suitable representatives and the intended trial participant/patient population might be involved in the development e.g. demonstrated usability (such as UAT).” |  |
| 1361 |  | **Comment:** In ePRO systems, the hand-held systems given to trial participants do not have audit trail enabled. Also, the date and time captured is each time the entire form is saved or submitted. In this sentence it is not clear if date and time capture expectation is at each field level or at the entire form level.  Is the intention here that participants should be able to access all of their data, such as device data and also everything that is entered into a clinical database, all the time? This would not be feasible in almost all cases during a clinical trial. Device data such as PROs and sensors offer more potential for immediate access for a defined period of time, however, there is a risk of bias for patients having access to previously entered PRO and diary data.  We support providing the participants access to data but would like to allow the data to be provided in alternative formats.  **Proposed change (if any):**  “Trial participants should ~~have access to~~ be able to obtain their own previously entered data, unless it is against the purpose of the clinical trial design or the protocol.” |  |
| 1363-1367 |  | **Comment:** Clarification of this text is suggested.  **Proposed change (if any):**  “Decisions about ‘view-period’ ~~for participants~~ should be based on considerations regarding risk for bias on data to be entered. ~~but also considering that~~ If view of recently entered data is not possible by the participant, then there is a risk that the participant could forget if relevant data have been collected. This isespecially the caseif the planned entry is not foreseeable ~~and~~ e.g., ~~just~~ requires ~~e.g.,~~ input once daily and is ~~but e.g.,~~ event-driven.” |  |
| 1368 |  | **Comment:** Clarification of this text is recommended.  **Proposed change (if any):**  “Logical checks should be in place to prevent unreasonable data changes ~~unreasonable~~i.e., “time travel” ~~e.g.~~ such as going back (months, years back in time) or forward ~~forth~~ into the future based on the protocol design.” |  |
| 1380 |  | **Comment:** This conflicts with the definition in the image below line 384. This seems to be inconsistent since data are not held on the device unless “offline” and then it is deleted as soon as sync occurs. |  |
| 1382 |  | **Comment:** Clarification is required with reference to *“source document”*. Is source document referring to the certified copy or source data as defined in prior sections? Source data ceases to exist on the device once the data is transferred from the device. We would suggest changing *“document”* to *“data”* to be consistent with prior text.  **Proposed change (if any):**  “The sponsor should identify the source ~~documents~~ data in the protocol and document the timing and locations of source document storage.” |  |
| 1384 |  | **Comment:** We would propose amending the text to clarify the timeframe.  It should be clarified if submission refers to data transmission to durable server identified in lines 1376-1783. If so, we would recommend the same term (i.e., data transmission) to avoid confusion.  **Proposed change (if any):**  “Besides the general requirements on audit trail (please refer to section 6.2), if an ePRO system is designed to allow data correction post user submission of patient data, the data corrections should be documented and an audit trail should record if data saved in the device are changed ~~before~~ after submission (if changeable).” |  |
| 1402-1404 |  | **Comment:** This section is fairly confusing. It seems to imply edit access for subjects, but then mentions at the end data changes are expected to be minimal. |  |
| 1402 |  | **Comment:** Please include documentation of the situation when a data originator realizes that they have submitted incorrect data by mistake.  **Proposed change (if any):**  “a procedure should be in place to address and documentthe situation when” |  |
| 1409-1412 |  | **Comment:** This statement *“it is not acceptable that data clarification procedures introduced by the sponsor or vendor whether or not described in the protocol do not allow for changes in trial participant data when justified e.g. if the trial participant realises that data has not been entered correctly”* is not clear.  Please clarify and simplify the text to make it understandable |  |
| 1417 |  | **Comment:** Please correct as proposed below.  **Proposed change (if any):**  “signed by the trial participant to avoid situations where ~~that~~ sites are manipulating data” |  |
| 1427-1428 |  | **Comment:** Please correct as proposed below.  **Proposed change (if any):**  Section heading for A5.1.1.5: “Contingency ~~Fall back~~ procedures and tracking of devices” |  |
| 1436 |  | **Comment:** A user email address is a typical identifier for a user, as it is for most online services (the email is used as a user ID, in that way the email user can be “verified” via an email to their account). To comply with this text currently would require that the user ID is a pseudo-random sequence of characters – this is bad user experience design. Also, comparing this text with line 1438 which requires attributability, it can only be achieved by using something personal to the user (e.g., an email address).  Please revise this text to account for the use of email as UID. |  |
| 1440 |  | **Comment:** There are no defined expectations for records of training.  Please state the expectations for user training records in this context. |  |
| 1441 |  | **Comment:** The term *“end user”* should be defined e.g., investigators, sponsors inspectors. |  |
| 1448-1451  Section A5.1.2 |  | **Comment:** Only clinician reported outcome is specified in the original draft. We would suggest revising this section to clinician reported outcome (ClinRO) and observer-reported outcome (ObsRO).  **Proposed change (if any):**  “Tools to directly collect clinician reported outcomes (ClinRO) or observer reported outcomes (ObsRO)should generally follow the same requirements as those described for systems in general. The main difference is the user (investigators, ~~other~~ clinicians or independent assessors for ClinRO; observers or caregivers for ObsRO ~~instead of trial participants~~), not the system requirements. Special attention should be given to access control in order to avoid jeopardising any blinding, when relevant.” |  |
| 1458-1459  Section A5.1.3 |  | **Comment:** We would suggest adding information on modes of administration/ devices of data collection if there are more than one way of data collection.  **Proposed change (if any):**  “It is necessary to provide alternative ways of data collection e.g. devices provided by the sponsor as the trial participants should not be excluded from a trial if not capable or willing to use BYOD. The mode of data collection is suggested to be documented when collecting data.” |  |
| 1462-1464  Section A5.1.3 1 |  | **Comment:** We would suggest adding more qualification activities (operating systems) for considerations.  **Proposed change (if any):**  “Qualification activities should also take things like upgrade of operating systems and different screen sizes into account e.g. for visual analogue scales (VAS)*,* or for questionnaires which require a bundle of questions to be displayed at a single screen*,*where the general presentation should be the same irrespective of device.” |  |
| 1478 |  | **Comment:** Clarification is required as to the application-level security access controls expected to be levied as in the absence of participants unique password or PIN to the device or to the application, there are no other options available to the application designer. |  |
| 1493 |  | **Comment:** The IP address is considered by GDPR as personal data.  Further clarification is required: the collection of BYOD-specific identifying information is in contradiction to data privacy/ confidentiality and might even pose a risk to unblinding; what and how many of such identifying data may be collected to meet ALCOA++ principles by - at the same time - ensuring data privacy and confidentiality? Does data privacy and confidentiality per se exclude BYOD from clinical trials? Please clarify.  **Proposed change (if any):**  “operation system (OS) details, browser details, screen size, ~~IP address,~~ international mobile equipment” |  |
| 1522 |  | **Comment:** *“Ownership of the clinical trial application and data should be specified”*: what is expected here exactly? Are we requested to mention that sponsor owns the app and data is collected through it? In what document should this be mentioned? |  |
| 1524 |  | **Comment:** *“published separate a”* is not correct.  **Proposed change (if any):**  “The GCP-IWG published separately a reflection paper on use of IRT in clinical trials.” |  |
| 1528 |  | **Comment:** Dose calculation based on individual entries is a crucial step for the integrity of the data of a clinical trial and the safety of the trial participants. One should add that these IRT (interactive response technology) systems have to be validated based on a risk-assessment and considering human factor aspects of the intended user group.  Please consider adding that these IRT systems have to be validated based on a risk assessment and considering human factor aspects of the intended user group. |  |
| 1538 |  | **Comment:** In certain scenarios, it may be possible for a blinded scientist to guess whether a subject has received a drug or placebo based on physiological changes observed that are not necessarily adverse events. An example is when a blinded cardiologist observes obvious ECG changes after dose administration. It does not truly break the blind because it is only a guess. It would be helpful to address what this means in the context of blinding here to eliminate ambiguity. |  |
| 1547 |  | **Comment:** As this refers to *“paper approach”*, clarification is requested as to whether this option is in scope of this guidance. |  |
| 1555-1556 |  | **Comment:** In the IRT system, all the data needed are recorded at the time of randomization. Once the randomization transaction has been performed, these data should not be changed anymore (so the data are fixed in the IRT database at the time of the randomization). This principle allows the analysis to be performed as per randomization. If we correct the data after randomization transaction, it will no longer be possible to perform the analysis as per randomization.  **Proposed change (if any):**  “In such cases, the additional functionality and GCP requirement concerning eCRFs should be addressed in the IRT system requirements and UAT~~. For example, investigator control of site entered data, authorisation of data changes by the investigator, authorisation of persons entering/editing data in the eCRF by the investigator~~, but only before the randomization transaction, so as to perform an analysis as per randomization.” |  |
| 1570-1572 |  | **Comment:** This section requires further clarification as eICFs are required to be reviewed by IRBs/IECs at the site level which requires compliance with the country regulatory agency requirements. |  |
| 1588-1589 |  | **Comment:** There is no basis for calling out e-consent as more likely to bias who participates than any other aspects of a trial design/conduct that may make some people more or less likely to participate.  We recommend the Agency removes inappropriately speculative and discouraging use of a particular aspect of technology that is almost ubiquitous in society today. |  |
| 1591-1592 |  | **Comment:** The protocol should not detail the format of the consent. By following the recommendation of the Agency, we are exposing the protocol to unnecessary deviations when alternative mechanisms are invoked in a contingency situation or create unnecessary addenda to accommodate country specific regulations.  **Proposed change (if any):**  “~~Any sole~~ The use of electronic informed consent should be ~~justified and~~ described either in the protocol or in other essential documents retained by site and sponsor.” |  |
| 1592-1594 |  | **Comment:** The use of the eConsent should not eliminate the face-to-face communication between the trial participant and the site. We recommend addressing in-person and remote communication methods in this paragraph.  Clarification on the possibility of obtaining the consent remotely is advisable, especially for initial consent for pre-screening activities, low interventional trials (under EU 536/2014 Clinical Trial Regulation) or informed consent amendments or addenda that may not warrant the patient being on-site.  Could face-to-face communication include the use of video (Microsoft Teams/ ZOOM, referring also to lines 1602-1603), e.g., for decentralized clinical trials and in the pandemic scenario. If so, we would suggest to specify this.    **Proposed change (if any):**  “Face to face communication (in person or via telehealth) between one or more members of the research team and the potential trial participant is considered essential and could in some countries be mandatory at least for some specific situations (e.g. due to the characteristics of the disease or of trial).” |  |
| 1594 |  | **Comment:** Please avoid using the word *“could”* to provide clarity. Please include details of where this requirement is mandatory as this helps sponsors implement systems which are compliant and not interpreted to be non-compliant. It would also be helpful to clarify the use of the term *“could”* as this then means that innovation stops as it is considered mandatory in all 27 Member States. |  |
| 1603 |  | **Comment:** *“nationally”*: Should this be *“legally”* or *“based on local regulations”* or something similar? Is that decision made at the country level or at the state/province level?  In addition, please correct the sentence as follows.  **Proposed change (if any):**  “this can be justified and is ~~where~~ allowed nationally” |  |
| 1604 |  | **Comment:** We recommend adding examples (e.g., televisits) to this sentence instead of the words for *“two-way communication in real time”*. It is difficult to understand the intent of the sentence as it is currently written. |  |
| 1618 |  | **Comment:** Clarification on the requirement for the informed consent form to be *“personally dated”* is required. This approach would reduce the benefits of electronic informed consent that eliminates potential mistakes related to date entering as occurs with wet-signature processes.  Duplication with ICH GCP should be removed as it is not required. Considering that E6 is undergoing revision, outdated principles of personally writing in dates when electronic tools are being used should be updated in E6 to provide more accurate date (i.e., trial participants can easily enter the wrong date, whereas a validated computerized system will not capture the wrong date). |  |
| 1623-1629 |  | **Comment:** This section demonstrates why manually entered dates in electronic informed consent forms is a redundant process and creates unnecessary burden on the participant. Whilst this may reflect the current wording of ICH GCP, it is not future proofing a guidance which will soon be outdated when ICH GCP is updated. |  |
| 1623 |  | **Comment:** *“country”*: is this controlled at the country level or something more local? |  |
| 1631 |  | **Comment:** Clarification is required as to how, where remote source data verification of informed consent forms is not allowed, monitors, auditors and inspector should access informed consent forms signed electronically. |  |
| 1634 |  | **Comment:** It is not clear if this requires the trial participant to be onsite or the actual documentation. However, many trial sites do not host their own IT systems so even evidence of a patient’s identity may not reside at the actual site.  We recommend that the agency clarifies what additional documentation should be retained for electronic consent that is not already retained for paper consent to enable identification of the person signing (patient or legal representative).  **Proposed change (if any):**  “~~It should always be possible to verify the identity of a trial participant with documentation at the trial site.~~ The identity of the trial participant should be verified with documentation available to the investigator.” |  |
| 1641 |  | **Comment:** We recommend that the agency considers removing this sentence. It appears in isolation and it is difficult to interpret without added context.  **Proposed change (if any):**  “~~Instead of an electronic signature, a biometric method may be considered.~~” |  |
| 1645-1648 |  | **Comment:** Clarification is required as to whether remote access to personal identifiable information in the electronic consent system is not permitted to all types of sponsor representatives such as CRAs or auditors. CRAs will require full access to verify patient identity and for the medical records.  Moreover, operationally, it is a challenge to have different types of access. It is therefore suggested that guidance on how this remote access to personal identifiable information should be provided by the CRAs as well as which related measures should be put in place.  Sponsor CRAs and auditors need to be able to verify valid consent was obtained. For many electronic systems (cloud based) this could only be via ‘remote’ access to an econsent system so a change is suggested to make it clear that only limited authorized sponsor personnel should be permitted to securely access personal identifiable information, especially given the current pandemic environment. In line 1675 and section 6, it is stated that access should be possible for regulatory authorities, so the capabilities for secure access to this data must be a feature of the system and available for review. |  |
| 1654-1655 |  | **Comment:** Written should no longer be a requirement when videos, pictures and story boards could easily one day take the place of a text-based form.  **Proposed change (if any):**  “Potential trial participants (or, where applicable, their legal representative) should be provided with access to ~~written~~ information about the clinical trial prior to seeking their informed consent.” |  |
| 1656 |  | **Comment:** We recommend that examples are added to this sentence for clarification purposes (e.g., video or transcript, link to glossary etc.). It is difficult to address the expectations of *“including all accompanying information and linked information”* without examples. |  |
| 1661 |  | **Comment:** Written should no longer be a requirement when it can be provided electronically to the patient.  **Proposed change (if any):**  “The trial participants should also be provided with a copy of their signed and dated ~~written~~ informed consent form (either electronically or on paper).” |  |
| 1062-1071 |  | **Comment:** Please consider simplifying by stating the Authorities expectations of testing (especially in view of FDA’s CSA Guidance document which is planned to be published). |  |
| 1662 |  | **Comment:** Clarification of the meaning of the term *“directly”* is required in this context e.g., directly from the application. |  |
| 1666-1667 |  | **Comment:** Essential documents should be available in the investigator TMF for their required retention period. |  |
| 1674-1676 |  | **Comment:** Please consider the below modification to ensure investigators can also revoke access to the electronic informed consent system.  **Proposed change (if any):**  “The system used should ensure that the investigator can grant and revoke access to the electronic informed consent system to the regulatory authority for inspections and that such access does not require the sponsor's involvement.” |  |
| 1679 |  | **Comment:** Please correct the sentence as suggested below.  **Proposed change (if any):**  “The electronic informed consent information (electronic trial participant information and informed consent form) is ~~are~~ subject to updates” |  |

Please add more rows if needed.