30 August 2017

Submission of comments on *Draft guideline for the notification of serious breaches of Regulation (EU) No 536/2014 or the clinical trial protocol – EMA/430909/2016*

Comments from:

| Name of organisation or individual |
| --- |
| EFPIA – Sini Eskola (sini.eskola@efpia.eu) |

*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)* |
| --- | --- | --- |
|  | EFPIA welcomes the opportunity to provide feedback on this important draft guidance. Our comments are rather extensive and this will hopefully help providing more clarity and improving the readability of the guidance. Where possible we've tried to provide a suggestion on how we believe the guidance could be amended to help the sponsors and other stakeholders to utilise the guidance appropriately as intended." |  |
|  | The primary objective of this guideline is to enable the concerned Competent Authorities to be aware of and ensure adequate follow-up of serious incidents in the trial  1. Clarity is needed about whether information from serious breach reports and follow-up should be made publicly available in the Database and, if so, how this would be done. Any process should deal with the parallel needs of protecting of personal data & commercially-confidential information and ensuring content is meaningful to those addressing the case itself, i.e. Sponsor and Competent Authority.  2. The timing of any public availability would also be a factor considering how any such information would be relevant to protecting public health and Article 81(4 & 5) of the Regulation.  3. Changes to the functionality of the Portal and Database may be needed to address these concerns  Recommended reasonable approach-  • Determine whether or not serious breach information must be publicly available according to the Regulation. If so:  • Consider whether all reported cases must be available or just those confirmed as serious by the Competent Authority.  • Consider appropriate timing and make changes to the Database design if necessary to enable control, e.g. not available the case is closed by the Sponsor and Competent Authority. Alternatively, does the current EU framework for Freedom of Information requests offer an appropriate process for reasoned requests for access? That would also allow for as-needed redactions as referred to below.  • Address protection of personal data & commercially-confidential information, e.g. in online reporting form and any redaction process that would be needed, including by which party. This should preserve necessary details needed at the time a new case is being assessed and followed up by the Sponsor and Competent Authority but not appropriate for public access. |  |
|  | **Readability of the guideline-**  For enhanced readability, suggest a re-structuring of this guidance to a more logical flow and also to ensure that titles/subtitles align with the content of the text.  e.g. Current Part 5- General considerations when reporting. …. Could be placed after the “Scope” and before “How to report serious breach”.. Also current section 4. “How should the breach be notified “ could be part of How to report serious breach. The new sequence could look like…  Table of contents   1. Legal requirements 2. Scope 3. General considerations *(include here lines 111-118 and lines 85-90)* 4. How to report a serious breach   4.1. What needs to be reported *(include here what is currently under 5.1, i.e. lines 120-148)*  4.2. Who should notify the serious breach? *(include here what is currently under 3.1, i.e. lines 50-53)*  4.3. When should the notification be made *(include here what is currently under 3.2, i.e. lines 54-83)*  4.4. Serious breaches occurring outside the EU/EEA *(include here  lines 91-108; title of chapter changed to match content)*   1. Responsibilities of parties involved in the notification of a serious breach *(currently part 6)*   5.1. Sponsor  5.2. Investigator/third parties  5.3 Retention   1. General expectation for serious breaches *(currently part 7)* 2. References   No details are existing currently here what is planned..see further comments below |  |
|  | **Section 2 Scope-**  **Third bullet point**- **is to outline actions that may be taken by the EU/EEA member states concerned in response to the notifications..**  Details of this and how procedure will be manged by EU/EEA member states are missing**.** No information is currently captured on this except lines 205-206  MS assessment of the serious breach - will this be a centralized assessment by the rMS to avoid multiple assessments and potential delays in the conduct of the study. More details about the assessment would be welcome.  Referring to the regulation just as reference will not be helpful. |  |
|  | **Section 3.2 Reporting timelines [ day 0] and days counting.**  Line 55 states, “within 7 calendar days of the sponsor (or anyone contracted by the sponsor) becoming aware of the breach”. Line 60 state “date of first awareness of a **serious** breach”. Line 67 and 68 both refer to “**serious** breaches”. Line 70/71 state “**reasonable grounds to believe** that a **serious** breach has occurred”. Line 75 states “confirm that a serious breach has actually occurred”.  Please consider when issues are notified first they are potential serious breaches and need to be assessed to see if they meet the criteria of reportability. This is not the same as the efforts to collect follow up information for the purposes of follow up reports to the initial breach report but rather to ascertain if the issue is reportable or not. The aim is to cut down on over-reporting or incorrect reporting of Potential breaches that do not meet the criteria for reporting and increases the burden on the assessor at the agency.  It is not possible to comply with the 7 calendar days from awareness of **potential** breach. one suggestion -the most efficient way to manage this- is to start the 7 days from the date of identification of a **reportable** breach – NOT the date the potential breach is sent for investigation and assessment of reportability.  - In many instances a breach needs further investigation to confirm if the serious breach criteria is met. In this scenario, the reporting timeline i.e. day 0, should be triggered from the date of confirmation.  ***A pragmatic approach to clock start should be employed.***  Proposed change (if any): *This comment refers to line* 60.  ~~In this circumstance day 0 (i.e. the day of first awareness that a serious breach has occurred) would be the date when the third party is informed.~~  *In this circumstance Day 0 (i.e. the day of first awareness* ***of information*** *that* ***provides reasonable grounds that*** *a serious breach has occurred) would be the date when the third party is first informed.*  OR  “In this circumstance day 0 (i.e the day **clear and unequivocal evidence that a serious breach has occurred is obtained**) could be the date when the third party is informed.  -The current MHRA process has the step of reporting “Potential SBs” to the MHRA – they then decide if the event was in fact an SB or not. This step does not seem to exist in the EMA process so it seems EMA is relying on the assessment by the Sponsor. Will there be any feedback from the EMA when reporting will be done, regarding their agreement or disagreement of the Sponsor assessment? |  |
|  | **Section 4-Line 96- Draft guidance states: “Serious breaches are notified through the EU CT system. All relevant fields must be completed. “**  AS part of this guidance, is it possible to provide information on what the relevant fields will be in the EU CT system? Perhaps include as an Appendix? This would help assist companies to align their internal processes and fully comply with reporting expectations.  **Section 4- mentions** that in some instances notifications need to be not only under **Article 52, but also Article 53 or Article 54** as applicable. This is further combined with whether the breach occurs within or outside the EU/ EEA, whether it affects patient safety, affects data in a CT application under review, impact on reliability and robustness of data, and impact on risk/benefit.  This complexity is perhaps better rendered/illustrated in diagrammatic format.  It would be helpful if the guideline could specify whether independent notifications are required or whether there will be only a single notification for which the exact scope is specified before submitting via the portal (e.g. by ticking all applicable CTR articles).  The same applies to **section 7** (reporting of serious breaches also under **Article 42**) |  |
|  | **Section 6- Responsibilities of the parties involved-**  can this alsohavea sub section on  -EMA responsibilities/actions similar to the MHRA serious breach guidance.  -Lead member states and other concerned member states responsibilities and expected actions  also section 6.3 on retentions is odd here unless this is seen as part of the responsibilities and hence included here.It can also be part of general expectations. |  |
|  | **Section 7**  General expectation for serious breaches includes some examples of what might constitute serious breaches (e.g. overdose in relation to an error), which are also reflected in appendix I. If examples are included in section 7 then it is important that they are completely consistent with the examples cited in annex I to avoid any confusion or misinterpretation |  |
|  | **Appendix I** [see also specific examples at the end of the document]  - The Guideline for notification of serious breach is intended to give guidance on what would and wouldn’t be considered a serious breach, however limited examples are provided in Appendix I to address when a breach scenario is not met. This is particularly important in order to avoid unnecessary serious breach reporting. In many instances a breach needs further investigation to confirm if the serious breach criteria is met.  - It would be helpful if the guidance could further clarify, in some of the examples, whether there is an assumption that these events occurred within the EU/EEA or exclusively outside, and how that difference would affect the requirement to report.  - It would be helpful to include clear justification in each example that connects the recommendation for whether the situation was a serious breach to one of the defined criteria for serious breach. This would aid companies in following the logical thought path from event to criteria.  - Line 70 talks about reasonable grounds.. can one provide more details on what is considered as reasonable in appendix?  -overall lines 71 to 76 –text could be simplified to have more clear message.  - Section 7, General expectation for serious breaches includes some examples of what might constitute serious breaches (e.g. overdose in relation to an error), which are also reflected in appendix I. If examples are included in section 7 then it is important that they are completely consistent with the examples cited in annex I to avoid any confusion or misinterpretation  - Some of the examples in the Appendices lack enough detail and context to demonstrate whether or not they could be serious breaches. Sometimes, this is only apparent in the explanation on the right or in relation to some subsequent event, such that enforcement action was later taken. e.g. The safety events should not be counted as GCP breach unless they are a GCP breach. An example is overdose in oncology. An overdose is customary reported as SAE. Adding the need for a serious breach report will create confusion and besides, it may not be a serious breach because the maximum dose administrable for many oncology drugs is above the one used in late stage studies and is defined in the phase 1 as an MTD. An increase of, say, 10% in dosing it is highly unlikely to have an effect on the safety of the patient, yet it would require a double reporting (SAE and serious breach).  e.g. **Potential Fraud**  There is insufficient detail to establish the case as potential fraud. The fact that enforcement action followed later does not help with the initial assessment by the Sponsor, which would not know that at the time. The reference to paediatric studies is not helpful as it does not relate to the definition of a serious breach, which applies to all clinical trial types equally.  **Proposed change (if any):** Update the scenario to establish e.g. that no reasonable explanation could be established for the discrepancies or irregularities and that fraud remained a possibility.  Comment: SAE Reporting  The second example is not clearly written: the number of events concerned and their impact on the safety profile of the product are not clear given the few details set out.  The third example lacks the detail to establish it as a serious breach with respect to either immediate subject safety or data reliability, e.g. the number or proportion of unreported AEs, were they unreported AEs or SAEs? The context of impact on dose escalation is only made apparent in the rationale, not the original scenario.  Proposed change (if any): Update the examples to include the context that clearly represents any serious breaches. |  |
|  | **General – Serious Breach - Data Integrity**  Assuming a trial is running exclusively in the US, so no patients from EU are affected. However, it could be that the data of the trial will also be submitted at some point in EU.  Could you kindly confirm whether this is outside of the Serious Breach scope (since the trial is not running in any EU country), or whether it might still qualify as Serious Breach in case these data should be used for submission in any pertinent country?  Defining serious breach at the level of one patient rather than focusing on structural issues that have an impact on patients and data will likely result in a process that does not add value because of the potential high amount of cases that will be reported.  For an issue occurring at a single investigator site for a single patient a Sponsor QMS root cause analysis and full-blown CAPA process do not make sense from a risk management perspective.  The above approach negates the direction provided by ICH-GCP revision to have a risked based approach. Please clarify alignment with risk based approach as described in ICH E6 revision |  |

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)* |
| --- | --- | --- | --- |
| §1 Legal Requirement  *Line 39* |  | Comment: *:” 2. For the purposes of this Article, a ‘serious breach’ means a breach likely to affect to a significant degree the safety and rights of a subject or the reliability and robustness of the data*  *generated in the clinical trial.”*  Proposed change (if any): Would rather state it as serious breach if it did affect to a significant degree… (cfr App II initial assessment : line 213 : question is whether the breach does affect to a significant degree the safety of subject etc…) |  |
| 65-67 |  | Guidance states: “If the notification function has been delegated by the sponsor to another party, for example, a CRO, the 7-day timeline applies to the other party”.  Suggested edits for emphasis/clarity: “If the notification function has been delegated by the sponsor to another party, for example, a CRO, the 7-day timeline still applies ~~to the other party~~ to both parties, regardless of who first becomes aware of the breach. |  |
| 68 |  | “which results in the serious breach being reported to the to the Member States”  Comment: Typo  Proposed change (if any remove duplicate to the |  |
| Line 77-83 |  | Comment: Further guidance is needed on the process to downgrade a case if the additional investigation indicates that that serious breach criteria is not met. Direction is required on how to rescind a notification and close out the report. |  |
| Line 79 |  | Comment:  Article 52 of Regulation 536/2014 refers to EU portal for notification, the guidance should be consistent in nomenclature to avoid potential confusion.  Proposed change (if any):  ..the sponsor shall permanently update the information in the EU ~~database~~ **portal**) |  |
| Lines 87-90 |  | Comment: Article 53 requires notification within 15 days of sponsor awareness. Article 54 requires notification within 7 days of measures being taken. Sponsors should be able to make a single submission fulfilling all relevant articles. For example, if notified under Article 52, a separate notification should not be needed under Article 54 or Article 53 if applicable. This will streamline reporting for sponsors and avoid confusion of the differing timelines since Article 53 has a 15-day notification period.  Proposed change (if any):  For serious breaches that are likely to affect the benefit/risk balance of the trial, in addition to the reporting requirement under Article 52, the sponsor **should indicate in the same notification if** ~~has to consider~~ the reporting requirement under Article 53, as an unexpected event, or Article 54, as urgent safety measure, **is also met, if** ~~as~~ applicable. |  |
| Lines 87-90; 100-105 |  | Comment: Multiple notifications should be avoided, notably with unexpected event, in order not to duplicate the information and facilitate the communication with the Member states. Serious breaches would be in essence an unexpected event. |  |
| 91-95 |  | Comment: In paragraph 91-95 which describes the requirement to withdraw a CT application under evaluation in the EU/EEA if a serious breach occurs outside the EU/EEA, it would be helpful to clarify if only withdrawal of the CT application is necessary in this case, or if any further requirements to communicate this serious breach to the MSC are required.  There could be a scenario where the CTA does not require withdrawal and therefore recommend language to allow for this scenario.  also.. a single patient safety serious breach has an impact on accurateness but might not have an impact on the robustness/interpretation and therefore we should not withdraw the application and in line with article 52. so suggestion to add word significant  Proposed change (if any):  If a serious breach occurred outside the EU/EEA while the application for CT authorisation is under evaluation in the EU/EEA territory and the serious breach has **a Significant** impact on the accuracy or robustness of data filed in an application dossier, the sponsor should **consider** withdraw**ing** the application and correct the aspects or data impacted, as applicable (in case for example the serious breach resulted from the problems in the design of the CT). |  |
| 91-95  97-99  100-105 |  | **Comment:** These are all cases of SBs occurring outside of the EU/EEA  **Proposed change:**  Further emphasis of such cases could be included in a dedicated subparagraph (e.g. 4.1) |  |
| Line 96  **Comment on line 96-99:** |  | Comment: Article 52 of Regulation 536/2014 refers to EU portal for notification, the guidance should be consistent in nomenclature to avoid potential confusion.  Proposed change (if any):  Serious breaches are notified through the EU ~~CT system~~ **Portal**  [ identify and mention relevant fields needed in the process]  The Regulation (Art 26) allows discretion by the Member State regarding the language in which a Clinical Trial Application is submitted but accepting a language commonly understood in the medical field is encouraged. Given the very short time available to Sponsors to assess and submit notifications of serious breaches, giving Sponsors the discretion to submit in either local language or a suitable common language would help them to meet their obligations promptly. This reflects the practical challenge international sponsors have in compiling and assessing cases across multiple countries. |  |
| 96 |  | “Serious breaches are notified through the EU CT system. All relevant fields must be completed.”  Comment: It is assumed that there will be a form to complete and therefore the possibility to comment on it prior to release as well, especially if it is different from the current MHRA notification form <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275216/Notification_of_serious_breaches_of_GCP_or_the_trial_protocol_form__1_.doc>.  This template will be important for the reporting party in order to track elements such as breach identification date by sponsor, notification date, initial or follow up etc.  Proposed change (if any): EMA to circulate the serious breach form to understand which fields will need to be completed. |  |
| 97-99 |  | Comment:  Amend to bring in line with serious breach definition within the CTR.  Proposed change (if any):  *Serious breaches occurring exclusively outside the EU/EEA that might have an impact on* ***~~data integrity~~ robustness and reliability of data generated in ~~of~~*** *a CT already authorised or being conducted in the EU/EEA territory, should be notified to the MSC under the reporting requirement of Article 52.* |  |
| Lines 97-99 and 197-199 |  | Comment: For the same context of serious breach occurring exclusively outside the EU/EEA, why is there a difference in the use of ‘might have an impact on data integrity’ in the case of reporting to the MSC and ‘significant impact on the integrity of overall data’ for notification to the EU system?  Proposed change (if any): Proposal to move lines 197-199 after line 99 and clarify, or merge these lines. |  |
| 100-103 |  | Comment:  Remove additional text to align with definition of a serious breach included in the CTR.  Proposed change (if any):  *Serious breaches of the protocol of an EU/EEA authorised clinical trial occurring outside the EU/EEA that are likely to affect the safety and the rights of a subject* ***enrolled in ~~and/or the benefit/risk balance of~~*** *a CT already authorised or being conducted in the EU/EEA territory, should be notified to the MSC under the reporting requirement of Article 52.* |  |
| 100-105 |  | Comment: Assume that line 101 reflects 'the safety and rights of a subject inside the EU/EEA?'  This is inferred in the next line down (102) but could be more clearly stated. We would recommend further clarification that a serious breach occurring outside the EU/EEA impacting a subject inside the EU/EEA must be reported according to Article 52 requirements. This is confirmed later in lines 197-199.  Edit proposed to line 101 for clarity.  **Proposed change (if any):**  Serious breaches of the protocol of an EU/EEA authorised clinical trial occurring exclusively outside the EU/EEA that are likely to affect the safety and/or the rights of a subject inside the EU/EEA and/or the benefit/risk balance of a CT already authorised or being conducted in the EU/EEA territory, should be notified to the MSC under the reporting requirement of Article 52. |  |
| Lines 100-105 |  | Comment: For the same context of serious breach occurring exclusively outside the EU/EEA, why is there specificity for serious breaches of the protocol compared to other serious breaches?  Explanation needed?? |  |
| After Line 105 |  | Comment: Please add whether and how a serious breach should be reported for completed trials if detected after the end of the trial. |  |
| Lines 100-105 |  | Comment: To avoid duplicate reporting, Sponsors should be able to make a single submission fulfilling all relevant articles. For example, if notified under Article 52, a separate notification should not be needed under Article 53 or Article 54 if applicable. Propose delete instructions to also report under Article 53 or Article 54 as addressed in line 87-90.  Proposed change (if any):  Serious breaches of the protocol of an EU/EEA authorised clinical trial occurring exclusively outside the EU/EEA that are likely to affect the safety and the rights of a subject and/or the benefit/risk balance of a CT already authorised or being conducted in the EU/EEA territory, should be notified to the MSC under the reporting requirement of Article 52. ~~In addition the sponsor has to report 103 according to Article 53 as an unexpected event or an urgent safety measure (according to the 104 requirement of Article 54), as applicable.~~ |  |
| Lines 106 - 108 |  | Comment: More clarification is wished on which kind of substantial modification this refers to.  **Proposed change:** Replace the generic term substantial modification with a specific definition (protocol amendment, modification of the application, depending on what applies) to get more clarity.  Also This paragraph is misplaced or it should not be considered as a particular point of this paragraph.  Proposed change (if any): Move this sentence after line 69. |  |
| 111-112 |  | Guidance states: “The majority of these instances are technical deviations that do not result in harm to the trial subjects or significantly affect the scientific value of the reported results of the trial”.  “Technical” seems to be vague choice of word. Perhaps use of the term “minor” or “administrative” deviations would be better description or perhaps delete the word “technical” altogether. |  |
| 111-116 |  | In addition, these deviations should be included and considered when he clinical study report is produced, as they may have an impact on the analysis of the data. However, not every deviation from the protocol needs to be reported to the EU CT system as a serious breach.  Proposed change:  In addition, these deviations should be ***~~included and~~*** considered when he clinical study report is produced, as they may have an impact on the analysis of the data. However, not every deviation from the protocol needs to be reported to the EU CT system as a serious breach.  Rationale: only significant and relevant deviations are included in the CSR. Technical/ non-significant deviations are not included in the CSR. |  |
| 111,192 |  | ***Consistency question:***  Are the references to "GCP" in lines 111 and 192 intended given that "Regulation" is referred to in lines 36, 85, 121 and 182? |  |
| 120-126 |  | Comment: Pls clarify if safety and rights; reliability and robustness is meant or if safety and/or rights; reliability and/or robustness is meant. For instance, in many of the examples listed in Appendix I the safety of the subjects is likely to be affected but not the rights. |  |
| Line 122 |  | Comment: This wording would benefit for further refinement and definition. There are many deviations to protocols but in order to know which should be reported further language is needed to identify the consequence of the deviations. The follow on language addresses this but as it is not linked to the first bullet this reads as two stand-alone set of criteria. They should be linked to give the right backgrounds to consider of the deviation meets criteria for reporting or not.  Proposed change (if any): “b) **Any serious breach of** the version of the protocol applicable at the time of the breach.” |  |
| 123-128 |  | **Comment:** “A serious breach is a breach which is **likely** to affect to a significant degree...”  “The judgement on whether a breach is **likely** to have a significant impact on the scientific value of the trial depends on a variety of factors …”  We would like to change the phrase “likely to affect” in a more robust statement to avoid unnecessary notifications  **Proposed change:**  “For the purposes of this Regulation, a serious breach is a breach which ~~is likely to~~ **adversely** affect ~~to a significant degree~~: (a) The safety and rights of a subject...”  “The judgement on whether a breach is ~~likely~~ to have a significant...” |  |
| 127-128 |  | Guidance states: “For the purposes of this Regulation, a “serious breach” is a breach which is likely to affect to a significant degree:  (a) The safety and rights of a subject.  (b) The reliability and robustness of the data generated in the clinical trial.  The judgement on whether a breach is likely to have a significant impact on the reliability and robustness of the data ~~scientific value~~ of the trial depends on a variety of factors.”  Suggest to replace ‘scientific value’ [line 127] with the term ‘reliability and robustness of the data’ to explicitly reference the prior paragraph [line 126, item (b)] |  |
| 133-136 |  | Comment: This example mentioned under 5.1 is slightly different to what is mentioned in Appendix I under IMP 3). Would it still be a Serious Breach, even if the subject did not experience an AE? It would be good to add both cases to the Appendix I.  Examples of potentially conflicting examples:  A single overdose in a single patient without any safety effects would be considered as a serious breach versus 182-186 an overdose which results in a SUSAR could constitute a serious breach. The latter implies you need an adverse event as outcome the former not. |  |
| 133-136 |  | Comment:  Amend text to bring in line with the definition of a serious breach included in the CTR. Current text is confusing. Overall challenge with this example We would propose to strike this example out and/or add in the appendix I with correct explanation.  Proposed change (if any):  *In the same way, if one or more overdose(s) occurred due to a miscalculation, this would still meet the criteria for a serious breach* ***if it was likely to affect to a significant degree the safety of a subject*** *regardless of whether or not the subject(s) suffered adverse reactions as a result of that overdose.*  Comment: Please clarify if there is an expectation that all overdoses are reported as serious breaches regardless of impact to subject safety (e.g. results in AE or SAE). Also, in the situation noted, if correct dose calculation instruction was included in protocol and site training but the overdose was caused by staff error is serious breach reporting required?  Examples in Appendix I of a yes and no scenario would be helpful. |  |
| 137-138 |  | Same comment as above. Guidance States: “It is the responsibility of the sponsor to thoroughly perform a root cause analysis to identify the cause of the serious breach and to assess the impact of the breach on the reliability and robustness of the data ~~scientific value~~ of the trial”.  For consistency, suggest to replace ‘scientific value’ with the term ‘reliability and robustness of the data’ to explicitly reference wording in line 126, item (b). |  |
| 140-142 |  | Q1- where the information is expected to be document? TMF file? elaborate in line 140.  ***Q2-***  will the sponsor need to submit the corrective and preventive actions to the portal? Suggest to specify whether it will be possible to update the serious breach form (f.e.as a follow up note to the original notification) or will there be a need to submit a new form to document the CAPA?  Q3- Line 140- As ‘appropriateness’ is subjective any details or explanation on criteria to evaluate the appropriateness of the decisions and actions taken by the sponsor could be helpful. This could be precised in section 6. Responsibilities of parties for instance. |  |
| Line 144 |  | Comment: The sentence is not clear as it gives the impression that the reporting of serious breaches is not always mandatory.  Proposed change (if any):”this may help when deciding on whether to ~~submit~~ **consider an event as** a serious breach ~~notification”~~. |  |
| 147-148 |  | Comment:  Amendment to text to provide clarity that notification of serious breaches can be delegated  Proposed change (if any):  *It is the sponsor’s responsibility to assess the information and ensure appropriate reporting****, even if notification of reporting has been delegated to a third party.*** |  |
| 155 |  | “patient(s) harmed or put at risk”  Comment: “Subject” is used throughout the document except here, “subject” is more appropriate due to vaccines and phase I.  Proposed change (if any): “subject(s) harmed or put at risk” |  |
| Lines 162-165 |  | Comment: A CRO or vendor would be considered an extension of the sponsor as per lines 55-57 and section 3.2 already addresses the requirement to have contractual agreements and processes in place to report breaches. It would be better to have investigator and third party split into separate sections as the third party is an extension of the sponsor and should be considered under responsibilities for sponsor in 6.1.  Proposed change (if any):  ***6.2. Investigator/~~third parties~~***  The investigator **site**~~/third parties (for example, vendor, CRO or investigator site)~~ should also have a process in place to identify and notify the sponsor of the occurrence of a serious breach. This may be a formal standard operating procedure or a process detailed in the protocol or study-specific guidance. |  |
| 169-170 |  | 1. “ …copies should be retained in the TMF …:  Comment: Documentation resulting from sponsor’s investigations for serious breaches is not typically an essential document of the TMF and might be assimilated to audit related documents which are not maintained in the TMF.  Proposed change: to retain only duration of 25 years and can be archived by the sponsor’s quality assurance department (or other designated repository), like audit reports).  2. Proposal to Changing sentence like in the regulation EC No 536/2014.  Proposed change (if any):”However~~,~~ ~~as a minimum,~~ copies should be retained in the trial master file for **at least** 25 years **after the end of the clinical trial**, as stated in..”  3. Further clarification is wished if the documentation of cases that have been examined but not considered to be SB also need to be retained for 25 years. |  |
| 173-174 |  | Comment:  The proposed change would support those entities such as smaller investigator sites who may not have well established quality management systems in place.  Proposed change (if any):  *Serious Breaches should also feed into the quality management system* ***or equivalent process****, to ensure…* |  |
| 176-177 |  | Guidance states: “It is expected that all confirmed instances of clinical trial fraud, which the sponsor becomes aware of are reported as serious breaches”.  Other, current serious breach reporting requirements (e.g. MHRA) are more nuanced – suggest revision below:  “If the sponsor becomes aware of fraud or misconduct which is likely to have a significant impact on the safety and rights of trial subject(s) or the reliability and robustness of the data generated, a serious breach report should be made.”  This suggestion is made with the understanding that confirmed fraud would be duly managed by a clinical trial sponsor accordingly (e.g. no further use of the investigator, reporting to local Health Authority and/or IRB/EC as required). The suggestion is made as well due to the fact that, short of an admission, confirmation of fraud is most times difficult to definitively prove. Reporting of “confirmed” cases of fraud (based on individual sponsor definitions/thresholds of confirmation), could introduce additional legal/privacy ramifications if not officially proven in a court of law.  Proposed change (if any):  Change into: all confirmed or potential (as identified by the sponsor) instances of clinical trial fraud that occurs in the EU/EEA  -As Lines 197-199 already cover what to do if a serious breach is identified exclusively outside the EU/EEA |  |
| 178-180 |  | Comment: The term “Site” has not been used in the text, so it is not clear what this paragraph is referring to? |  |
| Lines 182-186 |  | Comment: This is difficult to quantify as not every example of missed SUSAR reporting results in a patient being put at risk. It is not clear from the example whether the intention is to address lack of investigator identification and reporting of SAEs or lack of sponsor reporting of SUSARs. Lack of investigator reporting of SAEs could indicate a systemic issue which potentially is a serious breach as covered in Appendix I. Missed SUSAR reporting by sponsor would require judgement as to whether there was an impact of benefit risk.  Proposed change (if any):  Revise language dependent on intent of example. |  |
| Lines 184-185 |  | Comment: The sentence is misleading.  Proposed change (if any): If failure to manage safety events~~, for example lack of SUSAR reporting,~~ results in trial subjects being put at a significant degree of risk, then this will constitute a serious breach, **for example in case of lack of SUSAR reporting.**  Comment: It is not clear from the example to whom the SUSARs have not been reported “….lack of SUSAR reporting, results in trial subjects being put at a significant degree of risk, then this will constitute a serious breach”. E.g. Is this is a reference to the sponsor’s submission to a site/EC or to the EudraVigilance database (line 187)?  Proposed change (if any): Clarify further the lack of reporting to whom? |  |
| 189 |  | “If the serious breach also resulted in a temporary/permanent halt to the trial…”  Comment: 1. It is unclear if this refers to the halt of the full trial or should be interpreted as a halt at the concerned trial site.  2. Which additional notification is needed? What needs to be submitted/approved the MSC exactly? |  |
| 192-194 |  | Persistent or systematic non-compliance with GCP or the protocol has a significant impact on the safety to be handled as serious breach. This contradicts earlier statements that one deviation potentially impacting one patient safety should be considered a serious breach.  Please clarify contracting sections. |  |
| 195 |  | Guidance states: “If a serious breach occurred at one investigator site leads to the removal of data from the trial analysis, then this should be notified accordingly”.  A few comments:   1. Please clarify here whether reference to serious breach “at one investigator site” is intended to apply if the breach occurs at a site “within” the EU/EEA, “outside” of the EU/EEA or “both”? (See similar comment for lines 100-103 above.) 2. What does “this should be notified accordingly”? Does this refer to reporting as a Serious Breach in the event that the data analysis has been completed and already submitted within the EU/EEA as part of a Clinical Study Report (CSR)/dossier under review? 3. Should one assume that this would **not** apply to situations where a Serious Breach outside of the EU/EEA occurs and the where final data analysis and Clinical Study Report (CSR) is still in progress and not yet submitted to the EU/EEA for review? In such cases, removal of data from the trial analysis would be disclosed accordingly in the CSR. 4. Does reporting as a Serious Breach apply to cases where “removal of the data” does not impact “the safety and rights of a subject” nor the “reliability and robustness of the data” overall? 5. Does “removal of data” also include cases where data from a site might be excluded (due to a Serious Breach) from a ‘primary’ analysis defined in the protocol but included in an alternate analysis/ sensitivity analysis? Assume yes but, for clarity, suggest that a parenthetical statement to this effect could be added. 6. Additional information is required on whether the trial is running in the EU/EEA to understand the example appropriately. 7. Sometimes serious breaches leading to the removal of data from the trial analysis, are only identified after Last Subject Last Visit of the trial. Reporting of serious breach to the Portal would then not have value.   Proposed change (if any):   1. If a serious breach at one investigator site leads to the removal of data from the trial analysis before Last Subject Last Visit of the trial, then this should be notified accordingly. If this is only determined after Last Subject Last Visit of the trial, the serious breach should only be documented in the CSR. |  |
| 195-196 |  | Comment:  Amend text to bring in line with serious breach definition in CTR  Proposed change (if any):  *If a serious breach occurred at one investigator site leads to the removal of data from the trial analysis, then this should be notified accordingly* ***if likely to affect to a significant degree the reliability and robustness of the data generated in the clinical trial.***  some further comments…  *1. Further clarification is wished if this is an additional notification as per the case described in 189-191 and whether this notification needs to be managed via the EU CT system also.*  2. This would normally take place as a follow up of investigations and action plan and would be reported in the CSR. Decision for a sensitivity analysis might be taken if a serious breach is confirmed but this analysis will normally be performed as part of the whole trial analysis for writing and publishing the CSR.  Proposal: It should be clarified that in such a situation disclosure of the removal of data from the trial analysis in the CSR is sufficient to satisfy notification requirements.  3. Need to specify if this concerns investigator sites located in any country or only in the EU/EEA.  This general statement that seems to cover sites located in any country is not consistent with line 197 to 199 that specifies that for breaches identified exclusively outside the EU/EAA, those that will require notification are those that have “a significant impact on the integrity of the overall data”. |  |
| 197-199 |  | Further clarification is needed on here.  Comment and Proposed change:  May be Delete these sentences as this is already described exactly in lines 100-105 |  |
| Page 10-last line |  | Page 10:visit date deviation is not considered serious breach since it is common deviation in clinical trials.  **Other common deviations** are incorrect ICF being signed by a single patient, Please clarify which such single events need to be reported |  |
| Line 207 Appendix |  | Comment: Emphasize that identification of serious breaches should be considered within their context of occurrence.  Proposed change (if any): “Examples of serious breaches (this is not an exhaustive list) **- Each case is to be assessed considering the context.”** |  |
| 207 Appendix |  | In the appendix, example on error in sample processing resulting in recruitment of more subjects to meet the endpoint is considered a serious breach because the subjects were dosed unnecessarily as a result of error in sample processing. It is not clear why this is considered as a serious breach since subjects were dosed mainly for the efficacy primary endpoint, which is still necessary. The error in the processing generally occurs several weeks after patients are sampled for blood and has no impact on safety. The modification to the protocol to increase sample size is normally submitted/approved by the health authority anyway. |  |
| 207 Appendix |  | In the appendix, example on Protocol compliance states that “Investigator site failed to reduce or stop trial medication, in response to certain laboratory parameters, as required by the protocol. This occurred with several subjects over a one year period, despite identification by the monitor of the first two occasions”. This is considered as serious breach because subjects were exposed to an increased risk of thrombosis. It is not clear in the guidance why subjects were at increased risk of thrombosis? Also it is not clear why this will be considered as a serious breach if the safety of the subject was not judged to be compromised by the investigator. |  |
| 207 (Appendix 1) |  | Examples of Serious Breach:  Line 207 Appendix 1 of the proposed guidance cites the “physical or mental integrity of trial subjects” and the “scientific value of the trial” as reasons for reporting issues as a serious breach.  The text appears to be taken from MHRA guidance on Serious Breach. These terms, however, are n*ot* used in the body of the EU regulation or in this draft guidance definition of a Serious Breach. |  |
| Appendix I  SAE reporting |  | SAE reporting example (page 11 - first example) needs some further explanations, as it would be the sponsor who makes the assessment whether an SAE is expected or not. |  |
| Appendix 1  Category SAE reporting |  | Comment  “The investigator was not clear on the reporting requirements for the trial and was incorrectly classifying events as expected, as they were common events seen with that particular disease.”  Comment and proposed action:  The assessment of expectedness to determine reporting requirements should be done by the sponsor not by the investigator. Hence in this example underreporting cannot be the result and hence this should not qualify as a serious breach although retraining of the investigator is required.  Therefore either remove this example or change the classification into “No”. |  |
| Appendix 1:  Category IMP / Dosing error reported  Example 1 |  | Details of breach reported mentions: “A subject was dosed with the incorrect IMP …” and response states it to be reportable: “**Yes,** there was significant potential to impact the safety or the right of trial subjects”.  There is a contradiction in this example as the issue is isolated to a subject and analysis states “impact on the safety or right of trials subject**s**”. Isolated issues are likely to not impact the safety or right of all subjects in a trial.  Proposed changes: “Yes” to the question of serious breach reportability should not be given for isolated errors with no magnitude to have a significant impact. This distinction should be illustrated in the example to clearly make a difference on this aspect. |  |
| Appendix 1 Example 2 |  | Comment: In this example two issues are described, first one patient being miss-dosed and then later an entire cohort. The discussion section does not make any differentiation between the two. Would the expectation be that the first event is reported as a SB and also the subsequent issue? |  |
| Appendix 1 Example 3 |  | Comment: subject was overdosed and experienced an SAE and should be reported as a SB. Given the potential inconsistent text included on the main body of the document it is suggested that the discussion box is further expanded to indicate if the SB criteria would be met if no SAE had occurred. |  |
| Appendix I - 207  Section IMP 2) |  | Comment: The example listed under 2) was copied from the MHRA listing, however, since the MHRA definition of a SB is differently worded, the first bullet point is not applicable (“physical and mental integrity of trial subjects”). |  |
| Appendix I - 207  Section IMP 3) |  | Comment: This example is slightly different to what is mentioned under 5.1 (line 133-136). Would it still be a Serious Breach, even if the subject did not experience an AE? It would be good to add both cases to the Appendix I. |  |
| Appendix I, IMP (3, overdose) |  | Comment: The current examples around overdose infer that the site administers the IMP.  For clarity, it would be helpful to also consider the example of a subject taking IMP at home who overdoses and suffers an AE and whether this may be considered a serious breach or not. |  |
| Appendix I - 207  Section IMP 4) |  | *“It should be noted that mitigation actions undertaken to remediate the occurrence of the breach (for example, but not limited to, a breach that led to the removal of data from the overall analysis) do not negate the fact that a breach occurred and should be treated according to the legal requirements. In the same way, if one or more overdose(s) occurred due to a miscalculation, this would still meet the criteria for a serious breach regardless of whether or not the subject(s) suffered adverse reactions as a result of that overdose.*  *4) A subject took IMP that had expired two days ago. The IMP was stable and the subject did not experience any adverse events and this issue was not likely to affect the data credibility of the trial.*  If a patient was taking expired IMP without SUSAR, rationale that this is no breach because no patient impact and because CAPA was implemented does not make sense since mitigation actions per previous text (131-136) do not have impact on decision of reporting as serious breach or not.  Please clarify conflicting information. |  |
| Appendix I - 207  Section IMP 5) |  | Comment: How could this potentially affect the safety of trial subjects? |  |
| Appendix I - 207  Potential fraud (page 9) |  | Comment: Discrepant to line 177, where is stated that only confirmed fraud needs to be reported as a SB. |  |
| Appendix 1 Potential Fraud (no numbers now provided in the document) |  | Comment: On two separate occasions the sponsor detected issues but there was not unequivocal evidence of fraud at the time of reporting. The discussion here is not so helpful and the example is potentially confusing. Based on the text in the main body “confirmed instances of fraud” should be reported as a SB. This example is very difficult to interpret or to apply, ie should an SB be reported when the first issue was detected, the second or both? Given that there is no equivocal evidence is this therefore not considered as confirmed?  In addition, does one of the trials being in a paediatric population have any bearing on the decision?  Proposed change (if any): In the examples indicated the relevant point in the decision and if multiple reports should have been made. |  |
| Appendix 1, page 10 – Emergency unblinding |  | Comment:  The example of the breach reported is given as “ *A clinical trial subject attended the hospital emergency department, that attempted to contact the hospital (using the phone number listed on the emergency card issued to the subject) in order to break the unblinding code. Pharmacy was unable to code break in a timely manner, as a result, the subject withdrew from the clinical trial feeling unhappy that the pharmacy was not available in an emergency situation”.*  The reference to the fact that the subject was *“Unhappy that the pharmacy was not available in an emergency situation”* be removed”, as it is stated in the example given that the pharmacy was available however they were unable to break the blind.  Proposed change (if any):  *A clinical trial subject attended the hospital emergency department, that attempted to contact the hospital (using the phone number listed on the emergency card issued to the subject) in order to break the unblinding code. Pharmacy was unable to code break in a timely manner, as a result, the subject withdrew from the clinical trial****~~feeling unhappy that the pharmacy was not available in an emergency situation~~****”.* |  |
| Appendix 1:  Category Emergency un-blinding |  | Details of breach reported mentions: “A clinical trial subject attended the hospital emergency department, that attempted to contact the hospital … in order to break the unblinding code. Pharmacy was unable to code break in a timely manner,  as a result, the subject withdrew from the clinical trial feeling unhappy…”.    As per above example, an isolated failure of emergency un-blinding is likely to not impact at all the course of treatment of a study.  Proposal: Example to be revisited to provide more clarity on the magnitude of the issue that would reach the cap for definition as serious breach. |  |
| Appendix I - 207  Protocol compliance  (page 10) |  | *Minor visit date deviation. A common deviation in clinical trials.*  The visit date deviation is not considered serious breach since it is common deviation in clinical trials.  Other common deviations are incorrect ICF being signed by a single patient.  Please clarify which of such single events need to be reported |  |
| Appendix I - 207  SAE reporting  (page 11) |  | ***“No,*** *if this did not result in other trial subjects being put at risk, and if it was not a systematic or persistent problem.*  *In some circumstances, failure to report a SUSAR could have a significant impact on trial subjects. Sufficient information and context should be provided for the impact to be assessed adequately. “*  It is understood that if one SUSAR is not reported this is not a serious breach because it was single event.  This implies that there first needs to be a trend.  Please clarify in which cases this would be a serious breach. |  |
| Appendix 1  Category SAE reporting |  | “The investigator was not clear on the reporting requirements for the trial and was incorrectly classifying events as expected” and then: “**Yes,** incorrect classification of seriousness criteria”.  Comment: “seriousness” is independent of “expectedness”. The example speaks about expectedness, the response speaks about seriousness which is inconsistent.  Errors from investigator sites on the assessment of events may occur, however investigators are not responsible for assessing expectedness which is based on the RSI as specified in the IB or approved label (SmPC). The pharmacovigilance department of the sponsor is responsible to evaluate the expectedness of an event against the RSI, and will then classify events as SUSARs when appropriate.  Proposal: Example to be corrected and modified.  “The investigator was not documenting all the AEs associated with the trial.”  Comment: “Documenting” can be ambiguous and misleading in this example. Sponsor would not know if something was not documented by the investigator but he can detect lack of reporting in the CRF through monitoring / SDV.  Proposed change (if any): “The investigator was not reporting all the AEs associated with the trial.” |  |
| Appendix 1, page 11 - SAE reporting |  | Comment:  The rationale for this example of serious breach is unclear – the example talks about the investigator classifying events as expected – but the rationale talks about SAEs being classified as AEs. The example and the rationale risk confusing the reader by mixing the concepts of expectedness and seriousness criteria. We proposed the section is re-worded to make clear the error was in expectedness assessment, consistent with the example in ‘Details of the breach reported’.  In addition, the section should be called ‘ADR’ reporting as only related events (ADRs rather than AEs) are reportable.  Proposed change (if any):  Section title  ***~~SAE~~ ADR*** *reporting*  Is this a serious breach column  *Yes, incorrect classification of* ***~~seriousness~~ expectedness*** *criteria, therefore* ***ADRs ~~SAEs~~*** *incorrectly classified as* ***~~AEs~~ expected,******~~or~~ resulting in*** *under-reporting of large numbers of SUSARs.* |  |
| Appendix 1: |  | **Comment**: It is recommended to provide more details and explanations on when a consent issue, fraud issue, emergency unblinding issue and randomization issue would constitute a serious breach. Additional examples would be welcomed. |  |
| Appendix 1  Category Randomisation/ stratification errors |  | “Patients incorrectly randomized/stratified according to the protocol.”  Comment: Isolated errors would not have a significant impact on the data or study overall.  Proposed change (if any): Modify the example to clarify that this is not an isolated but a recurrent deviation likely to have a significant impact on the overall data. |  |
| Appendix I |  | **Comment:** Only examples falling into the deviation from version of protocol are provided.  **Proposed change (if any):** Pleaseinclude some examples of departures from the regulation (EU 536&2014) that should be considered as SBs. |  |
| Appendix I |  | **Comment:**  Temperature monitoring  **Proposed change (if any):** Please include one example about records missing/not possible to be download from the electronic device used for temperature control |  |
| Appendix I |  | **Comment:**  Protocol compliance  **Proposed change (if any):** Further clarification is needed under what circumstances might ineligibility of a patient be considered a serious breach. |  |
| Appendix I |  | **Comment:**  Protocol compliance, example 2  **Proposed change (if any):** Further clarification is needed if this scenario should be considered as a SB due to recurrence.  Additional information on why or why not this was an SB would be useful. |  |
| 212-216 |  | The guidance here is contradictory, suggesting that there cannot be a serious breach if a corresponding assessment has not been made.  **Proposed change (if any):** “Has an initial assessment been made of the case as to whether it meets the definition of a serious breach? If so but it was inconclusive, can any further review be justified to establish whether it qualifies for reporting, bearing in mind that there should be no undue delay? If not, the incident remains a serious breach whilst this is investigated in full and therefore should be reported in the meantime. If clear and unequivocal evidence of a breach has been determined then this represents Day 0 with respect to notification.” |  |
| 213 |  | Comment: Assume that this statement should read “…degree the safety and/or rights of a subject” as opposed to “…safety and rights…”.  Proposed change (if any):  ….breach affects to a significant degree the safety and/or rights of a subject or the reliability…. |  |
| 214-216 |  | Comment: Lines 215-216 seem to partially contradict lines 214-215.  The intent of this section seems to be to state that a worst case scenario should be assumed - and the event considered and reported as a serious breach - until the investigation is complete and it proven otherwise.  Having this clarity of expectation would be helpful - clock start is one of the main areas of contention for organizations reviewing SBs under the current UK legislation  Proposed change (if any): |  |
| Lines 215-217 |  | Infers that a breach should be considered serious until deemed not. If this inference is correct this should be included earlier in the document (not in the Appendix). |  |
| 216-218 |  | Comment and Proposed action:  Add bold text  However, this may be difficult to determine initially and may take some time to investigate, but the incident remains as serious breach whilst this is investigated and therefore should be reported **when the investigation takes more than 7 days.** |  |
| 220 |  | Comment: Line 220 Have subjects been informed? We do not think it’s appropriate in the initial assessment stage to inform subjects as this is when information is being gathered and a full assessment underway. It is more appropriate for subjects to be informed where appropriate once the CAPA has been made and the EC informed potentially giving advice on how to inform the patients.  Proposed change (if any): Move the text in line 220 to the next section (CAPA). |  |
| 222-224 |  | Comment:  Why does the fact that the trial is part of an MAA or large scale academic trial have an impact on whether or not a breach is considered to be serious?  Propose to delete this paragraph. |  |
| Example 2) page 8/13 |  | Comment: For blind studies, this is only detectable after the unblinding not during the study. Does that mean that a serious breach has to be notified after the end of the study?  Proposed change (if any): “A subject was dosed with IMP **in an open-trial** from the incorrect treatment arm.” |  |
| Example 3) page 8/13 |  | Comment: In relation to the example mentioned in line 182, which states that an overdose in relation to an error resulting in SAE can constitute a serious breach but should not be considered systematically as a serious breach, please add another example of overdose not to be considered as a serious breach.  Proposed change (if any): |  |
| Appendix 1 Protocol Compliance (example 4) |  | Comment: No brain CT scan performed as part of eligibility. SB criteria met if this has an impact on patient safety. More discussion is justified here to give clearer guidance as to when the SB criteria are met and when it is not with respect to patient safety. If there is no clinical evidence of undiagnosed metastases in those subjects enrolled or a follow-up scan confirms the absence of metastases, it would be assumed the SB criteria would not appear to have been met? |  |
| Example 5) page 8/13 |  | Comment: It is unclear how this event could affect the safety of trial subjects. Is it the fact that the issue is systematic enough to be classified as a serious breach?  In addition, suggestion to move this example in the ‘IRT Issues’ category. |  |
| Example IRT issues page 9 |  | Comment: What would be the assessment if there is dispensing of expired IMP but no shortage of IMP? Please clarify if consideration should be given to the fact that there are multiple impacts for the trial. |  |
| Appendix I: Potential Fraud |  | Comment: The example would benefit from explaining what irregularities were identified to help better understand why this meets the criteria of a serious breach. |  |
| Appendix I: Source Data |  | Comment: It is unclear from the example at what point serious breach reporting was expected to have occurred, after the monitoring visit or after the audit. |  |
| Appendix 1 Source Data |  | Comment: two occasions are given here where concerns have been raised about changes to data (as part of the monitoring process and also following audit). It is not clear from the discussion section just at what point the SB criteria has been met and should be reported ie when detected by the monitor or only at the point that this has been verified by the auditor |  |
| Appendix I: Sample Processing - A cohort had invalid blood samples as they were processed incorrectly. |  | Comment: The example is open to interpretation as to whether serious breach criteria was met for the new patients who then needed to be enrolled or for the existing patients whose data was incorrectly processed. Further guidance is required as it is common to increase enrolment beyond original predictions e.g. due to eligibility failures, and this would not be interpreted to meet serious breach criteria. |  |
| Appendix 1 sample processing (example 2) |  | Comment: This example appears to mixing two situations together which have no clear relationship other than they relate to safety data. The discussion offers no perspective on either situation and simply states “yes” |  |
| Appendix 1  Protocol Compliance (example 2) |  | Comment: protocol compliance - Investigator site failed to reduce or stop trial medication, in response to certain laboratory parameters, as required by the protocol. This occurred with several subjects over a one year period, despite identification by the monitor of the first two occasions. This example does not help with any guidance on the expectation of timing for reporting the Serious Breach.  Proposed change (if any): Further clarification or guidance on the expected timing of reporting would be useful here. |  |
| Appendix I: Protocol compliance - Subject safety was compromised because repeat electrocardiograms (ECGs) |  | Comment: The example would benefit from an impact assessment in the column ‘Is this a serious breach?’. This example would aid understanding if the issues of ECGs not performed and inadequate quality control for interim safety reports for dose escalation were separated. |  |
| Appendix I: Protocol Compliance -  Investigator site failed to reduce or stop trial medication |  | Comment: Example would benefit from additional wording to reflect that the laboratory values indicated thrombosis.  Proposed change (if any):  Investigator site failed to reduce or stop trial medication, in response to certain laboratory parameters **indicating thrombosis,** as required by the protocol.  Is this a serious breach?  Yes,subjects were exposed to an increased risk of thrombosis **and the issue was systemic.** |  |
| Appendix I SAE Reporting |  | Comment: The example requires clarification as confuses the concept of expectedness and seriousness. An incorrect classification of events as expected by investigator would not impact whether the event was recorded as non serious or serious and therefore the breach rational is unclear. If information on expectedness has been provided by the investigator it can be taken into consideration by the sponsor when they assess the event against the appropriate RSI to determine if expected as per Article 42. This example would be better represented by using an example of incorrect classification by the investigator of serious events as non serious.    Proposed change (if any):  The investigator was not clear on the reporting requirements for the trial and was incorrectly classifying **serious** events as ~~expected~~ **non serious**, as they were common events seen with that particular disease. |  |
| Appendix I: Randomization/stratification errors |  | Comment: The examples would benefit from further information on the incorrect randomisation/stratification to aid interpretation. |  |
| Table on page 12  Examples Eg randomization error |  | Comment: if wrong subject got active vs placebo (eg 2 subjects were switched),  in the end the same amount of data has been collected, and no impact for subject safety => this would  not necessarily be a serious breach… so would be good to specify this might not always be the case, but then justification to be given. |  |
| Appendix II Line 215 - 217 |  | Comment: If the breach does not clearly meet serious breach criteria and an investigation is needed to confirm that a serious breach has actually occurred, the reporting timeline i.e. day 0, should be triggered from the date of confirmation.  Proposed change (if any):  However, this may be difficult to determine initially and may take some time to investigate, ~~but~~ the incident ~~remains as serious breach whilst this is investigated and~~ ~~therefore~~ should be reported **once serious breach criteria is met**. |  |
| L.209 Appendix II |  | Comment: please clarify the objective of this annex and add a reference in the core document.  Is it a guide? Is it a list that inspectors will expect to see in the assessment documentation? |  |
| Appendix II  Lines 212 - 217 |  | Comment: The following sentence is confusing “If not, then this is not a serious breach and should not be reported.” And seems to contradict the subsequent sentence “However, this may be difficult to determine initially and may take some time to investigate, but the incident remains as serious breach whilst this is investigated and therefore should be reported.”  Proposed change (if any): Consider removing the sentence indicating that a serious breach should not be reported. |  |