EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

13 December 2021
EMA/698382/2021
Quality and Safety of Medicines Department

Guideline for the notification of serious breaches of Regulation (EU) No 536/2014 or the clinical trial protocol

Draft adopted by GCP Inspectors Working Group (GCP IWG)	30 January 2017
Draft adopted by Clinical Trial Facilitation Group (CTFG)	31 January 2017
Start of public consultation	23 May 2017
End of consultation (deadline for comments)	22 August 2017
Final version adopted by Clinical Trial Facilitation Group (CTFG)	7 December 2021
Final version adopted by GCP Inspectors Working Group (GCP IWG)	13 December 2021
Date of coming into effect	31 January 2022

Keywords	***Serious breaches, sponsors, service provider, clinical trials, compliance, Regulation (EU) No 536/2014, protocol, clinical trial participants, assessment***

Official address Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
Address for visits and deliveries Refer to www.ema.europa.eu/how-to-find-us
Send us a question Go to www.ema.europa.eu/contact **Telephone** +31 (0)88 781 6000 An agency of the European Union

Table of contents

Glossary

Clinical Trial: means a clinical study which fulfils any of the following conditions: (a) the assignment of the trial participant to a particular therapeutic strategy is decided in advance and does not fall within normal clinical practice of the Member State concerned; (b) the decision to prescribe the investigational medicinal products is taken together with the decision to include the trial participant in the clinical study; or (c) diagnostic or monitoring procedures in addition to normal clinical practice are applied to the trial participants.

Sponsor: means an individual, company, institution or organisation which takes responsibility for the initiation, for the management and for setting up the financing of the clinical trial. For the purpose of this guideline, the sponsor can officially nominate *authorised delegates to perform the function of reporting Serious Breaches. This authorised delegates nominated by the sponsor can be, for example, a legal representative or contract research organisation (CRO).*

Service provider: means a party involved in the trial, for example, a CRO or other contracted organisation, with clinical trial related responsibilities delegated by the sponsor, other than the "delegated party" and "investigator", which could observe a breach and is requested to report it to the sponsor/delegated party; it can be, for example, a CRO, a vendor responsible for the interactive response technologies (IRT), the site/sites involved in the manufacturing of IMP.

Delegated party: a type of service provider, is a party delegated by the sponsor, through a written contract, to perform the tasks set out in Article 52 of Regulation (EU) No 536/2014, i.e. to assess incidents which could be suspected serious breaches and/or to report suspected serious breaches to CTIS on behalf of the sponsor.

Delegation of tasks does not remove the ultimate responsibility of the sponsor or investigator for the conduct of the clinical trial in accordance with the applicable legislation.

Investigator: means an individual overall responsible for the conduct of a clinical trial at a clinical trial site. If a trial is conducted by a team of individuals at a trial site, the investigator is the responsible leader of the team and may be called the Principal Investigator.

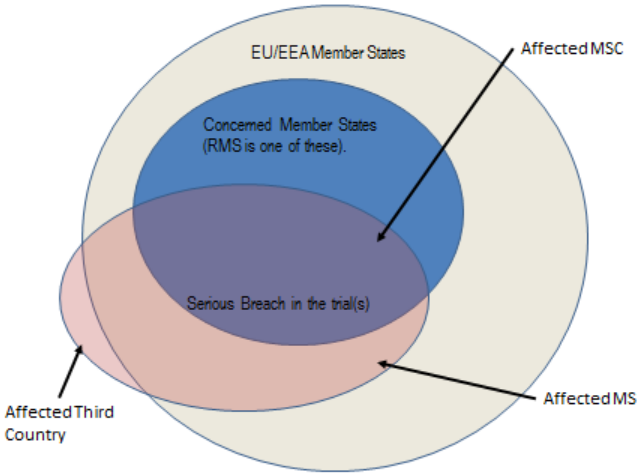
Suspected serious breach: means an incident which at the time of communication from investigators or from service providers to the sponsor has not yet been assessed by the sponsor to be a serious breach.

Serious breach: Any deviation of the approved protocol version or the clinical trial regulation that is likely to affect the safety, rights of trial participants and/or data reliability and robustness to a significant degree in a clinical trial.

Member State Concerned (MSC): means the Member State where an application for authorisation of a clinical trial or of a substantial modification has been submitted under Chapters II or III of the Regulation (EU) No 536/2014 respectively.

Reporting Member State (RMS): is the Member State Concerned elected in line with requirements of Article 5 of the Regulation (EU) No 536/2014, in the lead for the validation and assessment of part I phases.

Affected Member State (AMS): is the Member State directly affected by the serious breach. For example the Member State where the sponsor is based (as they have overall responsibility), the Member State where patients are affected by the breach, or it could be the Member State where the breach occurred (note this is not always a Member State concerned, as the breach could occur in an organisation in a Member States, i.e. an IRT provider, for a trial that has no sites in that Member State). Please refer to the figure below:



Disclaimer

This document was prepared in collaboration with the UK Medicines & Healthcare products Regulatory Agency (MHRA) and was available for public consultation between May and August 2017.

As of 1 January 2021 the UK is no longer a member of the European Union. Therefore, the MHRA published a national guideline on reporting serious breaches. Similarities in different sections can be identified between the UK and EU documents.

1. Legal requirement

Management of serious breaches of clinical trials authorised in the Europe Union (EU)/ European Economic Area (EEA) is defined by Regulation (EU) No 536/2014, which states in Article 52:

> *"1. The sponsor shall notify the Member States concerned about a serious breach of this Regulation or of the version of the protocol applicable at the time of the breach through the EU portal without undue delay but not later than seven days of becoming aware of that breach.*
>
> *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."*

2. Scope

To outline the practical arrangements for notification of serious breaches; this document does not cover notifications related to unexpected events, other reporting obligations related to the safety of trial participants or urgent safety measures, as defined in Articles 53 and 54 of the Regulation (EU) No 536/2014.

To provide advice on what should and what should not be classified as a serious breach and what must be reported.

To outline possible actions that may be taken by the EU/EEA Member States concerned (MSC) in response to notifications of serious breaches.

Serious breaches occurring in clinical trials authorised under the Directive 2001/20/EC cannot be reported through the EU portal and EU database - part of the Clinical Trials Information System (CTIS). In such cases, national requirements in place before the Regulation (EU) No 536/2014 became effective apply.

3. How to report a serious breach

3.1. Who should notify

The sponsor is responsible for the notification via the EU portal and EU database - part of the Clinical Trials Information System (CTIS). The sponsor may delegate this task to a service provider by means of a written agreement as described in Article 71 of the Regulation (EU) No 536/2014.

3.2. When should the notification be made?

Without undue delay and at the latest within **7 calendar days** of the sponsor becoming aware of a serious breach.

If the sponsor has reasonable grounds based on evidence to believe that a serious breach has occurred, it is expected to report the serious breach first, within 7 days, and investigate and take action simultaneously or after the notification. In this case, the sponsor should not wait to obtain all of the details related to the breach prior to the notification. In other cases, some degree of investigation and assessment may be required by the sponsor prior to the notification, in order to confirm that a serious breach has actually occurred. It should be underlined that according to the Regulation (EU) No 536/2014, only serious breaches must be notified, not suspected serious breaches. On the other hand, however, the sponsor should notify a serious breach without undue delay.

The sponsor should perform the assessment of a (suspected) serious breach in a timely manner from the moment they have received this information.

The sponsor should ensure, by means of a written contract that all parties involved in the conduct of the clinical trial, according to their area of responsibility, immediately report any events that might meet the definition of a serious breach to the contact point designated by the sponsor.

In the case of the principal investigator (PI), the protocol may take the place of a written agreement.

Documented training of the PI and site staff on this matter should be kept in the clinical trial master file (CTMF) and the sponsor should provide the PI with a dedicated, unique, e-mail address and telephone number for such communications that can be reached at all times.

The sponsor should review the received information and should make every effort to substantiate that the breach occurred was serious, before submitting it through CTIS. However, any assessment undertaken by the sponsor in order to confirm that the serious breach has actually occurred should not extend the reporting period of 7 calendar days.

Updates to the serious breach can be made whenever further information becomes available. If the investigation or corrective and preventive actions are ongoing at the time of reporting the serious breach, it is acceptable to indicate the plans with projected timelines for completion. In such case, it

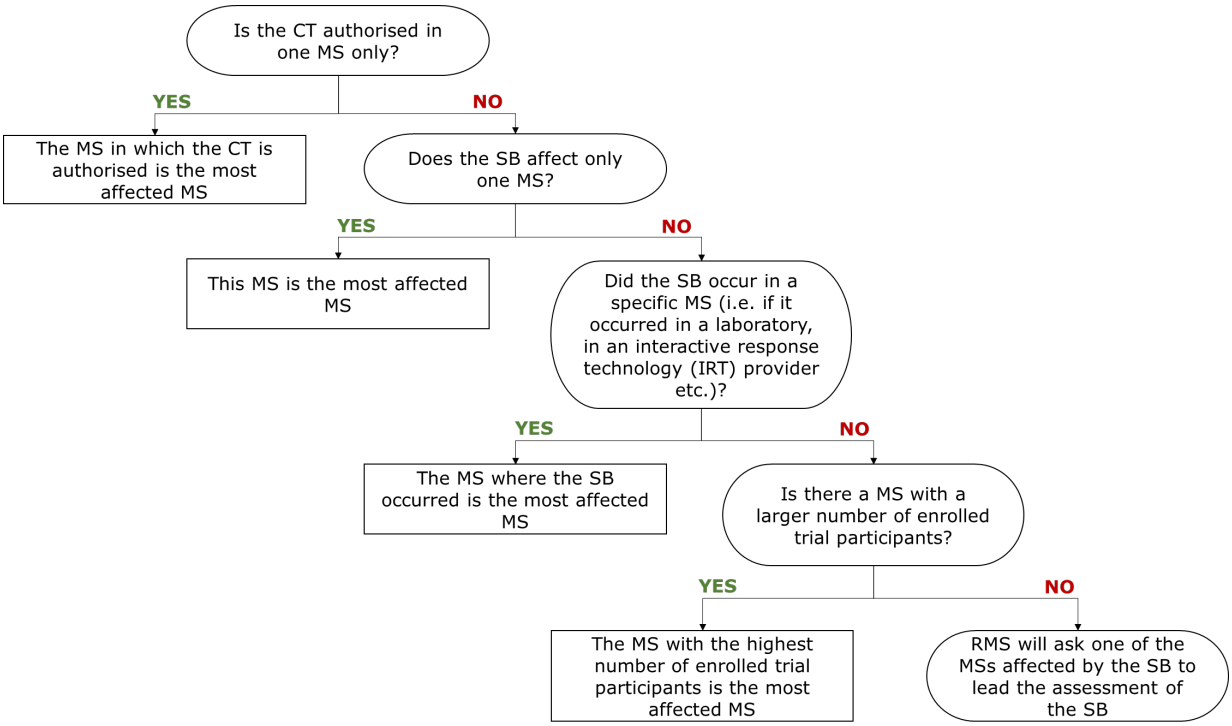
should be indicated in the initial report when these are expected to be completed and what follow-up reports will be submitted through the CTIS and when.

4. Clarification on reporting requirements

- Serious breaches which **occurred outside the EU/EEA** while the application for a clinical trial authorisation (CTA) **is submitted but not yet authorised** in the EU/EEA territory and the serious breach has an impact on the safety and/or the rights of a trial participant or reliability and robustness of data filed in an application dossier, the sponsor should address the concerns during the evaluation of the CTA. If this is not feasible or not satisfactory, this might lead to the withdrawal of the application via CTIS. If for example the serious breach resulted from flaws in the design of the clinical trial, the CTA may need to be withdrawn
- Serious breaches 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 trial participant or the reliability and robustness of the data generated in a clinical trial already authorised or being conducted in the EU/EEA territory, should be notified to the MSC via the CTIS under the reporting requirement of Article 52.
- When a sponsor notifies a serious breach, they should also consider if there are any other relevant notifications that need to be undertaken to comply with the Regulation (EU) No 536/2014, for example, requirements under Article 53 for unexpected events, or under Article 54 for urgent safety measures, or substantial modifications following a temporary halt or the decision to early terminate the trial under Article 37 and Article 38, respectively.

All relevant fields in CTIS, as presented in Appendix IIIa of this document must be completed. Unless the information reported in the CTIS fields is deemed exhaustive, the sponsor is encouraged to upload a report (using the "Add document" bottom) which should include all the details needed for AMSs/MSCs to assess the reported serious breach. To this purpose, the Appendix III b lists the topics which are expected to be covered. Sponsors should update the serious breach details in the CTIS fields and/or with a follow-up report if new information becomes available.

The sponsor should follow the below diagram and indicate which is the Member State most affected by the serious breach reported in the title of the notification and should report more details in Appendix III b.



5. Reporting serious breaches – Points to consider

5.1. What needs to be reported?

Any breach of:

- The Regulation (EU) No 536/2014.

or

- The clinical trial protocol version applicable at the time of the breach.

which is likely to affect to a significant degree:

- The safety of a trial participant.

and/or

- The rights of a trial participant.

and/or

- The reliability and robustness of the data generated in the clinical trial.

is serious and should be notified.

In line with Article 47 of the Regulation (EU) No 536/2014, the sponsor of a clinical trial and the investigators shall ensure that the clinical trial is conducted in accordance with the protocol and with the principles of good clinical practice.

The judgement on whether a breach is likely to affect the reliability and robustness of the trial data depends on a variety of factors, for example: the design of the trial, the type and extent of the data affected by the breach, the overall contribution of the affected data to key analysis parameters, the

impact of excluding the data from the analysis etc. It should be noted that mitigation actions undertaken to remediate the occurrence of the serious breach do not negate the fact that a breach occurred and should be treated according to the legal requirements.

In the same way, if a systematic and/or significant mis-dosing occurred, this would still meet the criteria for a serious breach regardless of whether or not the trial participant(s) suffered adverse reactions as a result of that mis-dosing.

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 trial data as well as the impact on a trial participant's safety and/or rights.

This assessment should be documented, as the appropriateness of the decisions and actions taken by the sponsor may be examined during any process triggered by the notification of the serious breach for example during GCP inspections.

Where the tasks of the sponsor have been delegated to a party, and a disagreement rises on classification/assessment of the breach between the sponsor and the delegated party resulting in no notification of a serious breach, the related communication between sponsor and delegated party should be documented. In particular, their respective individual position on whether or not a serious breach occurred should be recorded. In addition, the sponsor's reasons for not proceeding with the notification, whilst taking into account the views of the delegated party, should be documented.

Section 7 on 'General considerations for serious breaches' provides further information related to expectations for serious breach topics. This may help when deciding on whether to consider a breach as serious. Appendix I contains examples of situations that may be considered as serious breaches depending on the context of the situation. This list is not exhaustive and other types of serious breaches may occur. It is the sponsor's responsibility to assess the information and ensure appropriate reporting. Appendix II contains points to consider for sponsors in relation to the assessment of a breach.

Deviations from clinical trial protocols, good clinical practice (GCP) and/or European or national legislation may occur in clinical trials and where these are considered important, as defined by the ICH E3 guideline on the structure and content of clinical study reports, they should be described in the clinical study report (CSR). It is important to underline that an important deviation as defined in the ICH guideline E3 questions and answers (R1) is not equivalent to the definition of a serious breach and therefore an important deviation is not necessarily also a serious breach and vice versa. Nevertheless all serious breaches should be included in the corresponding clinical study report.

Deviations that do not significantly affect the safety and/or the rights of a trial participant or the reliability and robustness of the data generated in the trial should be documented (for example, in the trial case report form or the clinical trial master file) in order for appropriate corrective and preventive actions to be taken.

In addition, deviations considered important as defined by the ICH E3 guideline, even if they are not considered serious breaches, should be included in the clinical study report, as they may have an impact on the analysis of the data. However, not every (important) deviation from the protocol needs to be reported through the CTIS as a serious breach.

6. Responsibilities of parties involved in the notification of a serious breach

6.1. Sponsor

There should be a formal process in place to cover the legislative requirements of serious breach notifications. The following key points are to be considered:

- **suspected** serious breaches should be promptly reported to the sponsor by investigators and by service providers in order for the sponsor to perform further investigation and assess if the breach qualifies as serious breach;
- the management of the serious breaches should be included in the quality system of the sponsor, as a specific standard operating procedure and/or written in the protocol;
- after receipt, an assessment of the breach should be performed in order to establish whether it is "serious" (i.e. assessment of deviations/violations, isolated/systematic incident(s), trial participant(s) harmed or put at risk, data credibility etc.);
- an investigation of the serious breach, including a root cause analysis (this can be ongoing at time of reporting) should be performed;
- corrective and preventive actions should be identified (this can be ongoing at the time of reporting);
- reporting of the serious breach through the CTIS should be done within 7 calendar days of the sponsor becoming aware of a serious breach; lack of an adequate system in place and/or failure to report serious breaches may result in findings during GCP inspections (the grading will depend on the impact of the issue).

6.2. Delegated party

The delegated party performs the tasks set out in paragraph 6.1, as transferred by the sponsor as per written contract.

In addition, the delegated party keeps the sponsor informed about the management of all the breaches related to the clinical trials of that sponsor.

6.3. Service providers

Service providers (including service providers delegated by the principal investigator/institution):

- should have a written process in place to identify the occurrence of a (suspected) serious breach;
- should promptly communicate to the sponsor or delegated party a (suspected) serious breach, according to the contractual agreements stipulated and through the contacts (e-mail address or telephone number) provided by the sponsor or delegated party.

6.4. Principal Investigator

The principal investigator should have a process in place to ensure that:

- the site staff or service providers delegated by the principal investigator/institution are able to identify the occurrence of a (suspected) serious breach;

- a (suspected) serious breach is promptly reported to the sponsor or delegated party, through the contacts (e-mail address or telephone number) provided by the sponsor or delegated party;

This may be a formal standard operating procedure or a study-specific guidance.

7. General considerations for serious breaches

Due to the special nature of fraud it is expected that all concerns about potential cases of fraud in clinical trials which the sponsor becomes aware of are reported as serious breaches. National legislation must also be taken into consideration with reference to criminal acts.

The party (e.g. sponsor, CRO, investigator) at which the serious breach occurred should verify the impact of the breach on other clinical trials (ongoing or ended) where they are involved/ which they manage.

In some instances, a breach of the Regulation (EU) No 536/2014 or of the protocol (e.g. a mis-dosing in relation to an error) which may result in a Serious Adverse Event (SAE) or a Suspected Unexpected Serious Adverse Reaction (SUSAR) can constitute a serious breach. If failure to manage safety events, for example lack of SUSARs reporting, results in trial participants being put at a significant degree of risk, then this will constitute a serious breach which needs to be reported. This doesn't exempt the sponsor from the obligation to report, if relevant, other safety related notifications, as per the requirements of the Regulation (EU) 536/2014 (in accordance with Articles 53 and 54), in addition to the submission of those SUSARs to the EudraVigilance database.

If persistent or systematic non-compliance with the Regulation (EU) 536/2014 (including deviation from the principles of the GCP or the protocol as described in Article 47 of the same Regulation) is likely to significantly affect the safety and rights of a trial participant in the EU/EEA or on the reliability and robustness of the data of the trial, this will constitute a serious breach.

If a serious breach occurred at one investigator site within or outside of the EU/EEA for a clinical trial authorised/conducted also in the EU/EEA and this leads to the removal of data from the trial analysis, then this should be notified as well. Appendix I contains examples of situations that may be considered as serious breaches depending on the context of the situation.

8. Possible actions taken by the EU/EEA Member States concerned (MSC)

Serious breaches will be notified by the sponsors via the secure module of CTIS. After submission in CTIS this information will be visible in the secure module of the Member States that can perform an assessment. The assessment of the serious breach done by the Member States will lead to the publication of the serious breach and the corresponding evaluation done by the MS via the CTIS public domain.

Some of the serious breaches reported will be managed in-house via acceptable Corrective and Preventive Actions (CAPA) and with the oversight of the MS. Some serious breaches may require either an inspection and/or regulatory actions being taken.

Inspection request - the serious breach may trigger an (urgent) inspection. The outcome of this inspection may lead on to further regulatory action or even prosecution.
In case an inspection is deemed necessary, the notice of a serious breach will be published at the same time as the inspection report in CTIS, in line with section 4.5.3 of the Appendix on disclosure rules, to the "Functional specifications for the EU portal and EU database to be audited - EMA/42176/2014".

Regulatory actions - in case a serious breach requires regulatory actions to be taken, as for example corrective measures described under Article 77 of Regulation (EU) 536/2014, including revocation or suspension of the authorisation to conduct the clinical trial(s) or requiring the sponsor to modify any aspect of the clinical trial(s), these will be managed by the MSC. Except where immediate action is required, the MSC will ask the sponsor for their opinion. That opinion shall be delivered within 7 days.

Furthermore, actions with reference to national legislation might be applicable as well.

9. References

1. Regulation (EU) No 536/2014 of the European Parliament and the Council of 16 April 2014
2. Regulation (EU) No 536/2014 - Questions & Answers
3. Guideline for good clinical practice - ICH E6(R2) - EMA/CHMP/ICH/135/1995
4. ICH Topic E 3 Structure and Content of Clinical Study Reports (NOTE FOR GUIDANCE ON STRUCTURE AND CONTENT OF CLINICAL STUDY REPORTS (CPMP/ICH/137/95))
5. ICH guideline E3 - Questions & Answers (R1) - EMA/CHMP/ICH/435606/2012

Appendix I – Examples of serious breaches

This is not an exhaustive list and each case should be assessed individually, taking into account the context of the breach.

Category	Details of breach reported	Is this a serious breach?
1. IMP	1.1.1 A subject was dosed with the incorrect IMP administered via the incorrect route (the IMP used was from a completely different clinical trial to the one the subject was recruited to). 1.1.2 A subject was systematically not administered IMP doses by mistake, what may result in disease breakthrough or relapse. 1.1.3 A subject received/was administered IMP during pregnancy without having previously performed a pregnancy test required as per protocol, what may result in embryo-foetal toxicity.	**Yes**, it is likely to affect to a significant degree the safety and rights of a subject in the clinical trial. Such breaches may be caused, for e.g. by lack of training and may impact other subjects as well.
	1.2.1 A subject was administered the incorrect dose of IMP. In spite of CAPA implementation, some months later, the subjects in an entire cohort were incorrectly dosed with IMP three times daily when they should have been dosed once daily. 1.2.2 A subject systematically did not receive essential concomitant therapy described as per protocol, what may result in higher toxicity of IMP (e.g. oncology trials).	**Yes** • there was impact on the safety and rights of a trial subject or on the reliability and robustness of the data generated in the clinical trial; • this issue was systematic and persistent leading to a breach of the Regulation and the trial protocol; • this issue persisted despite the implementation of a corrective and preventive action plan.
	1.3.1 One subject was systematically administered additional doses of IMP. The subject was given instructions to take higher doses of IMP than what was stipulated in the protocol. The subject experienced a severe adverse event as a result. 1.3.2 One subject was mistakenly and repeatedly administered	**Yes**, there was impact on the safety and rights of a trial subject and on the reliability and robustness of the data generated in the trial. Even if the subject didn't experience an adverse event, the case is considered a serious breach because the dosing error was systematic and has an impact on the reliability and robustness of the data.

Category	Details of breach reported	Is this a serious breach?
	lower doses of IMP what may result in disease breakthrough or relapse.	
	1.4 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 was a single isolated incident.	**No**, there was no impact on the safety and rights of a trial subject or the reliability and robustness of the data generated in the clinical trial.
	1.5 A subject was harmed due to incorrect administration of the IMP as a result of incorrect instructions in the protocol.	**Yes**, as it affected the safety of the subject in the clinical trial. Moreover, subjects enrolled in the trial at other sites could be equally at risk. In this case, the breach would be relevant to EU/EEA sites and should be reported as a serious breach.
2. Temperature monitoring	2.1.IMP temperature excursions reported. 2.2 Compounded sterile IMP preparations were systematically administered after been stored in inadequate conditions.	**Yes**, if the situation was not managed and subjects were dosed with IMP assessed as unstable or where stability cannot be verified or reasonably assumed, which resulted in harm/potential to harm subjects. This is likely to affect to a significant degree the safety and rights of a subject in the clinical trial. **No**, if the excursions had been managed appropriately e.g. IMP was moved to alternative location/quarantined as necessary and a documented assessment (by qualified personnel) illustrated that there was no impact on subject safety and rights or reliability and robustness of the data generated in the clinical trial, and stability data showed it was stable.
3. IRT issues	3.1 Following a single incident of expired IMP being dispensed and in spite of CAPA implementation, multiple issues with the IRT system across several clinical trials occurred leading to the dispensing of expired IMP and a shortage of IMP at investigator sites in time of subject visits. 3.2 Due to an interactive response technologies (IRT) malfunction 50% of subjects assigned to one arm were	**Yes**, there was impact on the safety and rights of trial subjects and this issue persisted leading to a constant breach of the Regulation or the trial protocol, despite the implementation of a corrective and preventive action plan. **Yes**, this impacts the reliability and robustness of the data generated.

Category	Details of breach reported	Is this a serious breach?
	unblinded in a blinded trial, furthermore this information was submitted to all trial staff at all investigator sites participating in the trial.	
4. Potential fraud	4.1 On two separate occasions the sponsor identified issues with the same investigator site. First with consenting and then with suspected fraud in recruitment and consenting. However, there was not unequivocal evidence of fraud at the time of reporting. One of the studies involved paediatric subjects.	**Yes**, this is potential fraud that requires assessment and should be reported as a serious breach and investigation should continue in parallel to determine whether the fraud is confirmed. In this example, this breach subsequently led to legal action against the organisation in question.
5. Source data	5.1 Concerns were raised during monitoring visits about changes to source data for a number of subjects in a trial, which subsequently made subjects eligible with no explanation in the subject notes. An audit was carried out by the sponsor and other changes to source data were noted without explanation, potentially impacting on data integrity. Follow-up reports confirmed the sponsor concerns over consenting and data changes made to source without an adequate written explanation.	**Yes**, and this needs to be reported when, based on the concerns raise, the minimum information to assess that the case was a serious breach, were obtained.
6. Emergency unblinding	6.1 A clinical trial subject attended the emergency department, that attempted to contact the investigator site (using the phone number listed on the emergency card issued to the subject) in order to break the unblinding code. The unblinding process did not allow to code break in a timely manner.	**Yes**, as this is likely to affect to a significant degree the safety and rights of the subject if unblinding would have affected the course of treatment.
7. Sample processing	7.1 A cohort had invalid blood samples as they were processed incorrectly. As a result one of the secondary endpoints could not be met. Therefore, a substantial modification was required to recruit more subjects to meet the endpoint.	**Yes**, it is likely to affect to a significant degree the safety and rights of a trial subject as further additional subjects had to be dosed unnecessarily as a result of this error.
8. Protocol compliance	8.1 Subject safety was compromised because repeat electrocardiograms (ECGs) were consistently not performed, as required by the protocol. The ECGs were required as part of the	**Yes**, as it is likely to affect to a significant degree the safety and rights of a trial subject or on the reliability and robustness of the data of the clinical trial.

Category	Details of breach reported	Is this a serious breach?
	safety monitoring due to the pharmacology of the IMP. Also, there was inadequate quality control (QC) of the interim safety reports used for dose escalation which has potential for stopping criteria to be missed if adverse event (AEs) were not transcribed from the source to the safety report.	
	8.2 The thrombosis risk of an IMP was monitored by some laboratory parameters. Investigator site failed to reduce or stop trial medication, in response to altered values of these 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.	**Yes**, it is likely to affect to a significant degree the safety and rights of a trial subject as subjects were exposed to an increased risk of thrombosis.
	8.3 Major visit date deviation, based on impact assessment of trial participants safety and wellbeing and/or clinical trials data robustness and reliability (depending on the protocol). 8.4 Minor visit date deviation. A common deviation in clinical trials.	**Yes**, as this may have an impact on the trial participants safety and wellbeing and/or clinical trials data robustness and reliability. **No**, a minor protocol deviation, which does not meet the criteria for notification.
	8.5 According to the protocol, a brain CT scan should be performed in the selection visit in order to exclude brain metastasis (exclusion criteria). The site used a previous version of the protocol where the CT scan wasn't required so 6 patients out of 10 were included without brain CT.	**Yes**, because it shows lack of safety data collection. This exclusion criteria could potentially affect patients safety and rights and would affect the reliability and robustness of the data if the majority of patients were ineligible.
9. SAE reporting	9.1 The investigator failed to report a single serious adverse event (SAE) as defined in the protocol (re-training provided).	**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 SAE and as a consequence, failure of the sponsor to report a SUSAR could have a significant impact on trial subjects. Sufficient information and context should be documented for the impact to be

Category	Details of breach reported	Is this a serious breach?
		assessed adequately.
	9.2 The sponsor 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.	**Yes**, under-reporting of large numbers of SUSARs due to incorrect understanding of expectedness.
	9.3 The investigator was not documenting all the AEs associated with the trial.	**Yes**, depending on the type of trial, for example inadequate safety reporting in dose escalation studies may impact on the decision to escalate to the next dose level.
10. Consent	10.1 Patient information leaflet and informed consent updated, but at one trial site this was not relayed to the patients until approximately 2-3 months after approval.	**Yes**, if there was a systematic or persistent problem and/or if it has a significant impact on the safety and rights of a trial subjects (e.g. there was key safety information not relayed to subjects in a timely manner).
11. Access to data	11.1 The investigator would not allow sponsor/CRO access to the trial participants' notes.	**Yes**, it is likely to affect the safety and rights of a trial subject and the reliability and robustness of the data generated in the trial as the data could not be verified. The protocol should contain a clause to state that Sponsor representative and Regulatory authorities will have access to the data, and this is also reflected in the informed consent.
	11.2 Loss of data.	**Yes**, it is likely to affect the safety and rights of a trial subject and the reliability and robustness of the data generated in the trial. Clinical trial sponsors and vendors should have agreements in place addressing business continuity and ensuring that clinical trials data are retrievable at any point in time.
12. Randomisation/ stratification errors	12.1 Patients incorrectly randomized/stratified according to the protocol.	**Yes**, as this will be likely to have a significant impact on rights of the subjects or the reliability and robustness of the generated data.
13. DSMB/DMC	13.1 The Data and Safety Monitoring Board (DSMB)/ Data Monitoring Committees (DMC), which should be implemented according to the protocol and the clinical trial authorisation in a	**Yes**, the missing implementation of the DSMB/DMC is likely to affect to a significant degree the safety and rights of trial subjects and the reliability and robustness of the data generated

Category	Details of breach reported	Is this a serious breach?
	blinded trial, has in fact not been implemented.	in the trial.
14. Privacy	14.1 The Sponsor contracted a CRO to build an e-CRF – the e-CRF contained patient identifiable information. Both the Sponsor and CRO had access to all this information.	**Yes**, it affects to a significant degree the rights of a trial subject as it affects their privacy. Trial participant's confidentiality is a fundamental right by national requirements, by ICH-GCP and by ethical principles, which needs to be respected.
	14.2 A coordinating investigator site was sending follow-up questionnaires to trials subjects of other investigator sites (to save the other sites the extra work). For this they had the names and addresses of trial subjects of other investigator sites. The trial subjects were not informed about this and had not given consent for this. This does not affect subject safety but it does affect the privacy of trial subject.	**Yes**, it is likely to affect to a significant degree the rights of a trial subject as it affects their privacy.
	14.3 During an inspection, it was observed that the informed consent forms from trial subjects of one investigator site were being kept at another investigator site (also being the sponsor of the trial because it was an investigator initiated trial). The trial subjects affected were not informed about this and had not given consent for it.	**Yes**, it is likely to affect to a significant degree the rights of a trial subject as it affects their privacy.

Appendix II – Points to consider for sponsors in relation to the assessment of a breach

The aim of this appendix is to help sponsors to adequately identify and assess suspected serious breaches.

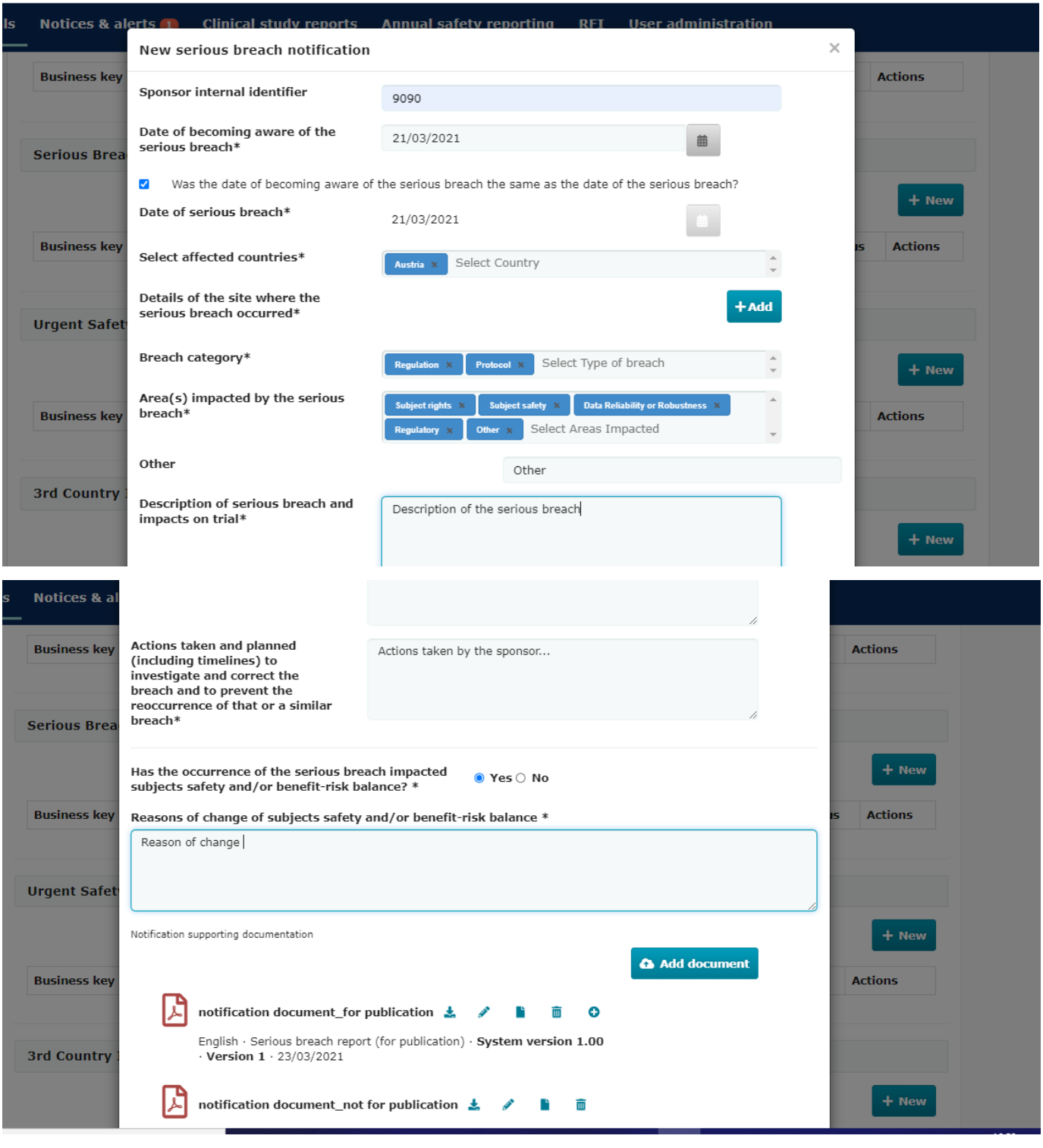
This is not an exhaustive list.

- It needs to be considered if the breach meets the definition of serious breach according to Art. 52 of Regulation (EU) No. 536/2014. This may be difficult to determine initially and may take some time to investigate. However, if the incident is likely to affect the safety and/ or rights of a subject to a significant degree or questions the reliability and robustness of the data generated in the clinical trial, then the incident should be regarded as a serious breach and reported as a serious breach during the investigation of the incident.

If there is a proper quality management system in place to ensure that:

- The sponsor can identify the root cause for a serious breach.
- The extent of the issue is evaluated and in case of a systematic serious breach, assessed if it can potentially affect other subjects within the same trial and/or other trials.
- There is an assessment whether it was a genuine human error, or lack of training, or failure to follow a procedure.
- If the breach is caused by a service provider, the sponsor checks whether this serious breach affects any of the sponsor's other trials, whether open or closed, managed by the same service provider.
- If subject safety and/or rights has/have been compromised, proper risk proportional actions are taken, which may include informing the subjects affected about the serious breach.
- The CAPA plan ensures safety of the affected subjects, or the reliability of the data. It needs to be considered if the clinical trial needs to be suspended or terminated or the affected data will need to be removed from the clinical study report.
- The CAPA plan addresses the serious breach and ensures that measures are put in place in order to avoid reoccurrence.
- Internal procedures are updated, training provided, systems updated.
- The proposed timelines for the CAPAs are reasonable according to the serious breach.

Appendix III a – Template form for reporting serious breaches



Appendix III b – Information to be submitted with a notification of a serious breach

(Mandatory fields in CTIS to be filled in and additional information to be added either as free text or as a separate document uploaded in CTIS)

A. GENERAL INFORMATION		
A.1	Status of the investigation of the serious breach	Concluded ☐ Ongoing ☐ Estimated date of next follow up (if known):
A.2	Clinical trial title	
A.3	Type of clinical trial	Commercial ☐ Non-commercial ☐
A.4	Inclusion of the clinical trial in a regulatory procedure (marketing authorization / variation)	Please *specify if the clinical trial is part of a marketing authorization or variation application or if it is planned to be included in such an application.* *If included in a regulatory procedure, please specify the product and procedure number.*
A.5	Are other clinical trials impacted by the same serious breach?	No ☐ Not Known ☐ Yes ☐ If Yes, please specify the EU CTR number: *(The reporter is requested to indicate in this section if they are aware of other clinical trial(s), registered in CTIS, impacted by the same serious breach)*
A.6	Details of the site where the serious breach occurred	*Please fill in in CTIS also the contact details of the site (tel., email)*
A.7	MS most affected by the serious breach	*Please indicate the MS most affected by the serious breach. According to the decision tree described in section 4, if the clinical trial is authorised in one MS only, that MS is the most affected; otherwise, it is identified answering the questions below. Please include the name of this MS in the title of the serious breach report.* Does the serious breach affect only one MS? Yes ☐ If Yes, please indicate the AMS. No ☐ If No, please indicate the AMSs and answer to the next question. Did the serious breach occur in a specific MS (i.e. if it occurred in a laboratory, in an interactive response technology (IRT) provider etc.)? Yes ☐ If Yes, please indicate the MS. No ☐ If No, please answer the following question. Is there a MS with a larger number of trial participants (i.e. the MSC with the largest number of actually enrolled subjects or, in case no participants has been enrolled jet, the MSC with the largest number of proposed participants) Yes ☐ If Yes, please indicate that MS and the number of trial

		participants for each MSC. No ☐ If No, please justify; in this case, "No most affected MS" should be indicated in the title of the serious breach report.

B. DETAILS OF THE SERIOUS BREACH		
B.1	Brief description of the serious breach	*Please describe here the serious breach, or indicate reference to the CTIS field or to an attached document if the information is already described elsewhere in a comprehensive manner.*
B.2	(Potential) impact of the serious breach	*In addition to the areas impacted by the serious breach which are mentioned in CTIS, please indicate the sub-category (Consent Form / confidentiality / IMP / approval issues, etc.)*
B.3	Other relevant details / information	
C. DETAILS OF THE ACTION TAKEN/PLANNED *For each of the following sub-section if details are not known at the time of report, a statement of when they will be available and submitted as a follow-up report should be provided.*		
C.1	Impact Assessment	*The extent of the impact should be investigated and reported: full details of the impact assessment, what has been looked at and how this has been done i.e. methodology should be included here.*
C.2	Root Cause Investigation	*Describe the Root Cause Investigation and results/outcomes of this investigation.*
C.3	Corrective and preventive actions (CAPA) plan	*CAPA plan should include any actions already taken; for each action, the following should be reported: who is responsible for the action (Sponsor, CRO, CRA, site etc.), timeline for implementation, if already concluded or pending. The CAPA plan should also include how this incident will be documented in the TMF.*
C.4	Actual Impact	*The actual consequences of the serious breach should be reported, explaining for example, if the action partially or totally prevented the "potential impact" (reported in section B) from occurring, if corrective action are still possible to ensure safety of the affected trial participants, or to ensure the reliability of the data.*