EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

31 January 2017
EMA/430909/2016

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
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
Date of coming into effect	

Comments should be provided using this template. The completed comments form should be sent to gcp@ema.europa.eu

Keywords	***Serious breaches, sponsors, clinical trials, compliance, clinical trial Regulation (EU) No 536/2014, violations, protocol, regulation, patients, assessment***

30 Churchill Place ● Canary Wharf ● London E14 5EU ● United Kingdom
Telephone +44 (0)20 3660 6000 **Facsimile** +44 (0)20 3660 5555
Send a question via our website www.ema.europa.eu/contact

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

Table of contents

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; it does not include guidance related to urgent safety measures or other reporting obligations related to subject safety.
- 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.

3. How to report a serious breach

3.1. Who should notify the serious breach?

The sponsor or a person duly authorised by the sponsor to perform this function, if this function has been delegated by the sponsor to another party (for example, a legal representative or contract research organisation (CRO)).

3.2. When should the notification be made?

- Within **7 calendar days** of the sponsor becoming aware of the breach or of anyone that has contractual agreement with the sponsor (CROs, contractors, co-development partners, etc.) becoming aware of the breach. Contractual agreements between clinical trial (CT) sponsors and other parties should clearly stipulate that any non-compliance identified by third parties, are promptly reported to the sponsor in order for the sponsor to meet its legal obligations. 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 first informed.

  If a principal investigator is aware of the occurrence of a serious breach, then processes should be in place to ensure that such information is promptly reported to the CT sponsor in order for the sponsor to meet the legal obligations.

- 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. Therefore, sponsors and CROs need to ensure that there is a documented process in place for timely communication on serious breaches between the parties, which results in the serious breach being reported to the to the Member States concerned by day 7.

- If the sponsor receives information that provides reasonable grounds to believe that a serious breach has occurred, it is expected that the sponsor reports the breach first within 7 calendar days, investigate and take action simultaneously or after notification. In this case, the sponsor should not wait to obtain all of the details of the breach prior to notification. In other cases, some degree of investigation and assessment may be required by the sponsor prior to notification, in order to confirm that a serious breach has actually occurred but this should not extend the reporting period of 7 calendar days.

- Reporters are not expected to wait until all the information is available. Updates to the breach can be made as further information becomes available (in line with the requirement of Article 81 (9) that the sponsor shall permanently update the information in the EU database). If the investigation or corrective and preventative actions are on-going at the time of reporting the serious breach, it is acceptable to indicate the sponsor's/reporter's plans with projected timelines for completion. In such case, sponsor/reporter should indicate in the initial report when these are expected to be completed and what follow-up reports will be submitted to the EU CT system[1] and when.

4. How should the breach be notified

- Serious breaches of the Regulation or of the protocol of an EU/EEA authorised clinical trial occurring in the EU/EEA that are likely to affect to a significant degree the safety and rights of a subject or the reliability and robustness of the data should be reported according to Article 52. 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 has to consider the reporting requirement under Article 53, as an unexpected event, or Article 54, as urgent safety measure, as applicable.

- 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 an impact on the accuracy or robustness of data filed in an application dossier, the sponsor should withdraw 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).

- Serious breaches are notified through the EU CT system. All relevant fields must be completed.

- Serious breaches occurring exclusively outside the EU/EEA that might have an impact on data integrity 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.

- 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 according to Article 53 as an unexpected event or an urgent safety measure (according to the requirement of Article 54), as applicable.

- Organisations should also consider if there are any other relevant notifications that need to be undertaken to comply with the Regulation, for example if a substantial modification is required due to a temporary halt in the trial.

[1] EU CT system encompasses the EU CT portal and database

5. General considerations when reporting serious breaches

Deviations from clinical trial protocols and GCP may occur in clinical trials. 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. These cases should be documented (for example, in the trial case report form or the trial master file) in order for appropriate corrective and preventative actions to be taken. In addition, these deviations should be included and considered when the 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.

5.1. What needs to be reported?

- Any serious breach of:

  (a) The Regulation (EU) No 536/2014.

  (b) The version of the protocol applicable at the time of the breach.

- 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 scientific value of the trial 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 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.

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 scientific value of the trial as well as the impact on the subject’s safety and 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.

The section on general expectation for serious breaches reporting provides further information related to expectations for serious breach topics; this may help when deciding on whether to submit a serious breach notification. Appendix I contains examples of situations that may be considered 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.

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. This should include:

- receipt and assessment (i.e. assessment of deviations/violations by sponsor/delegate, isolated/systematic incident(s), patient(s) harmed or put at risk, data credibility etc.);
- investigation including a root cause analysis (this can be ongoing at time of reporting);
- corrective and preventative action (this can be ongoing at the time of reporting);
- reporting to the EU CT system;
- compliance with the 7 calendar day reporting timeline.

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. Investigator/third parties

The investigator/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.

6.3. Retention

Retention of documents regarding serious breaches applies to both sponsor and investigator/third parties. The location where an organisation decides to retain the documentation of serious breaches will depend on each organisation's quality systems and business need. However, as a minimum, copies should be retained in the trial master file for 25 years, as stated in Article 58 of the Regulation EC No 536/2014.

However, it is also important that the breach is circulated/made available to staff for inclusion of relevant information in the clinical study report or a publication. Serious breaches should also feed into the quality management system, to ensure that lessons are learnt and effective preventative actions are taken to reduce the risk of similar occurrences.

7. General expectation for serious breaches

It is expected that all confirmed instances of clinical trial fraud, which the sponsor becomes aware of are reported as serious breaches. The term "site" refers to any site or party involved in the trial, for example, a CRO (such as laboratories analysing samples from subjects) or other contracted organisation and not solely to investigator sites. National legislation must also be taken into consideration with reference to criminal acts such as fraud.

In some instances, a breach of the Regulation or of the protocol (e.g. an overdose in relation to an error) which results in Serious Adverse Event (SAE) or Suspected Unexpected Serious Adverse Reaction (SUSAR) can constitute a serious breach. 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. In this case a serious breach notification will need to be submitted in

addition to the submission of those SUSARs to the EudraVigilance database as per requirements of Article 42 of Regulation 536/2014.

If the serious breach also resulted in a temporary/permanent halt to the trial, an additional notification would need to be submitted to the EU CT system and a substantial modification would need to be submitted and approved by the MSC prior to re-start the clinical trial.

If persistent or systematic non-compliance with GCP or the protocol has a significant impact on the safety of trial subjects in the EU/EEA or on the scientific value of the trial, this will constitute a serious breach.

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 a serious breach is identified exclusively outside the EU/EEA that has a significant impact on the integrity of the overall data, or it is likely to have a significant impact on the safety of trial subjects in the EU/EEA, then this will require notification to the EU CT system.

For example if a subject was harmed due to incorrect administration of the investigational medicinal product (IMP) as a result of incorrect instructions in the protocol, then subjects at other sites in the trial 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.

References

Procedure for the management of serious breaches by the EU/EEA Member States including their assessment and the appointment of a lead Member State

207 # Appendix I – Examples of serious breaches (this is not an exhaustive list)

Category	Details of breach reported	Is this a serious breach?
IMP	Dosing errors reported:	
	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).	**Yes,** there was significant potential to impact the safety or the rights of trial subjects.
	2) A subject was dosed with IMP from the incorrect treatment arm. In addition, 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.	**Yes** • there was impact on the safety or physical or mental integrity of trial subjects or on the scientific value of the 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 preventative action plan.
	3) One subject was 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.	**Yes,** there was impact on the safety of trial subjects and on the scientific value of the trial.
	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.	**No,** there was no impact on the safety or physical or mental integrity of the trial subject or on the scientific value of the trial. In addition, the assessment of the breach identified this as a single episode and a detailed corrective and preventative action plan was implemented.
	5) Due to an interactive response technologies (IRT) malfunction 50% of subjects assigned to one arm were unblinded in a blinded trial, furthermore this information was	**Yes,** this could potentially affect the safety of trial subjects, and this was a systematic issue. **Yes,** this impacts the robustness and reliability of the data

Category	Details of breach reported	Is this a serious breach?
	submitted to all trial staff at all investigator sites participating in the trial.	generated.
Temperature monitoring	IMP temperature excursions reported.	**Yes,** if the situation was not managed and subjects were dosed with IMP assessed as unstable, which resulted in harm/potential to harm subjects. **No,** if the excursions had been managed appropriately e.g. IMP was moved to alternative location/quarantined as necessary and an assessment (by qualified personnel) illustrated that there was no impact on subject safety and data integrity, and stability data showed it was stable.
IRT issues	Multiple issues with the IRT system across several clinical trials leading to the dispensing of expired IMP and a shortage of IMP at investigator sites in time of subject visits.	**Yes,** there was impact on the safety 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 preventative action plan.
Potential fraud	On two separate occasions the sponsor identified issues with the same organisation. First with consenting and then with potential irregularities 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 subsequently led to enforcement action against the organisation in question.
Source data	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	**Yes,** and this needs to be reported when the concerns were raised. *Note: not all of the information was provided in the original notification, the sponsor provided follow-up updates.*

Category	Details of breach reported	Is this a serious breach?
	explanation.	
Emergency unblinding	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.	**Yes**, as this had significant potential to harm the subject if unblinding would have affected the course of treatment.
Sample processing	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,** subjects were dosed unnecessarily as a result of this error.
Protocol compliance	Subject safety was compromised because repeat electrocardiograms (ECGs) were not performed, as required by the protocol. The ECGs were required as part of the 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.	**Yes**
	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.	**Yes,** subjects were exposed to an increased risk of thrombosis.
	Minor visit date deviation. A common deviation in clinical trials.	**No,** a minor protocol deviation, which does not meet the criteria for notification.

Category	Details of breach reported	Is this a serious breach?
	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,** if this had an impact on patient safety.
SAE reporting	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 a SUSAR could have a significant impact on trial subjects. Sufficient information and context should be provided for the impact to be assessed adequately.
	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.	**Yes,** incorrect classification of seriousness criteria, therefore SAEs incorrectly classified as AEs or under-reporting of large numbers of SUSARs.
	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.
Consent	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. *More information on the potential consequences of the delay should have been provided.*	**No,** if this was not a systematic or persistent problem and if no harm to trial subjects resulted from the delay. **Yes,** if there was a significant impact on the integrity of trial subjects (e.g. there was key safety information not relayed to subjects in a timely manner).
Access to data	The investigator would not allow any party access to the patients notes.	**Yes,** the data therefore could not be verified. The protocol would usually 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.

Category	Details of breach reported	Is this a serious breach?
	Loss of data due for example to servers' breakdown.	**Yes,** 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.
Randomisation/ stratification errors	Patients incorrectly randomized/stratified according to the protocol.	**Yes,** as this will be likely to have a significant impact on the data.
DSMB/DMC	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 blinded trial, has in fact not been implemented.	**Yes,** the missing implementation of the DSMB/DMC has significant potential to impact the safety of trial subjects.

208

Appendix II – Points to consider for assessment of the breach

Initial assessment

- Does the breach meet the definition of serious breach? Has there been an assessment of whether the breach affects to a significant degree the safety and rights of a subject or the reliability and robustness of the data generated in the clinical trial? If not, then this is not a serious breach and should not be reported. 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.
- If the breach is caused by a third party confirmation should be obtained of any other trials that might be affected – whether open or closed.
- If subject safety has been compromised, have the subjects been informed, where applicable?
- Have any ethical issues arisen that may require discussion with the Member States?
- Is the trial part of a marketing authorisation application (or planned to be part of an application?), or is it a large-scale academic trial that could potentially change prescribing practice and therefore have an impact on public health?

Assessment of the corrective and preventive action (CAPA)

- Has the root cause been identified?
- Was it a genuine human error, or lack of training, or failure to follow a procedure?
- Is this a systematic issue – can it potentially affect other trials?
- Is corrective action possible to ensure safety of the affected patients, or to ensure the reliability of the data? Or will the affected data need to be removed from the trial?
- Is the preventative action acceptable? Does the preventative action address the breach and ensure that it will not happen again? Do procedures need to be updated, training provided, systems updated?
- How will the sponsor assess that the CAPA is effective?
- Are the timelines reasonable?