



# **GUIDANCE FOR THE NOTIFICATION OF SERIOUS BREACHES OF GCP OR THE TRIAL PROTOCOL**

## **Table of Contents**

A. Legal requirement.....	1
B. Purpose of the requirement.....	1
C. Purpose of this guidance .....	2
D. Arrangements for notification .....	2
E. Identifying serious breaches .....	3
F. MHRA Actions.....	5
G. Organisation Responsibilities.....	5
H. References .....	6
Appendix I - Expectation for Specific Serious Breach Topics.....	7
Appendix II Examples of Serious Breaches Notified to MHRA (this is not an exhaustive list) .....	9

### **A. Legal requirement**

Regulation 29A of the Medicines for Human Use (Clinical Trials) Regulations 2004 [Statutory Instrument 2004/1031], as amended by Statutory Instrument 2006/1928, contains a requirement for the notification of “serious breaches” of GCP or the trial protocol:

“**29A.** (1) The sponsor of a clinical trial shall notify the licensing authority in writing of any serious breach of -

- (a) the conditions and principles of GCP in connection with that trial; or
- (b) the protocol relating to that trial, as amended from time to time in accordance with regulations 22 to 25, within 7 days of becoming aware of that breach.

(2) For the purposes of this regulation, a “serious breach” is a breach which is **likely** to effect to a significant degree –

- (a) the safety or physical or mental integrity of the subjects of the trial; or
- (b) the scientific value of the trial”.

### **B. Purpose of the requirement**

The requirement was implemented in UK legislation in order to:

- Enhance the safety of trial subjects/patients by seeking to ensure that the licensing authority is promptly informed of such serious breaches, in order to take appropriate action in response to the breach; and/or
- To take the information regarding serious breaches into account when assessing future applications for clinical trial authorisation, and applications for marketing authorisation, which include data from trials affected by serious breaches.



### **C. Purpose of this guidance**

- To outline the practical arrangements for notification.
- 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 MHRA in response to notifications of serious breaches.

### **D. Arrangements for notification**

#### **Who should notify?**

The Sponsor or a person legally authorised by the Sponsor to perform this function (for example, a legal representative or contract research organisation (CRO)), if this function has been delegated by the Sponsor to another party. In accordance with Statutory Instrument 2004/1031 as amended by Statutory Instrument 2006/1928, the Sponsor retains legal responsibility even if the function is delegated (Regulation 3.12). The CRO is also legally responsible for compliance with the legislation in relation to functions delegated by the Sponsor to the CRO (Regulation 3.8). However, in the interests of subject safety, reporting should not be delayed by discussion over reporting responsibility.

#### **When should the notification be made?**

- Within **7 days** of the Sponsor becoming aware of the breach. 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.
- If the Sponsor retains the notification function, then it is recommended that agreements between the Sponsor and other parties involved in the trial, for example, CROs, contractors, co-development partners, investigators, should state that the other party will promptly notify the Sponsor of a serious breach (as defined in Regulation 29A) that they become aware of, in order for the Sponsor to meet their legal obligation. In this case, the clock starts when the Sponsor becomes aware of the serious breach.
- If the Sponsor obtains clear and unequivocal evidence that a serious breach has occurred (as defined in Regulations 29A), the default position should be for the Sponsor to notify the MHRA first, within 7 days, and 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.
- A pragmatic approach to clock start should be employed. Inspectors will review the process for notification during MHRA GCP inspections and delays in notification may be classified as non-compliance. If in doubt about whether and when to notify, contact the MHRA GCP Inspectorate.



### Who should be notified?

- Notify serious breaches to the MHRA GCP Inspectorate. Notifications should be sent to the following email address:

E-mail to: [GCP.SeriousBreaches@mhra.gov.uk](mailto:GCP.SeriousBreaches@mhra.gov.uk)

Organisations should also consider if there are any other relevant MHRA units that should be notified to comply with other legislation (for example, notification to the Clinical Trials Unit (CTU) if the breach constitutes an urgent safety measure or if a substantial amendment is required due to a temporary halt in the study or to the Defective Medicines Report Centre if the breach involves defective medicines or IMP recall etc.) NRES SOPs also require that the research ethics committee is notified.

- A template form for notifications of serious breaches to the MHRA is available on the MHRA GCP webpage (<https://www.gov.uk/guidance/good-clinical-practice-for-clinical-trials>). **It is strongly recommended that organisations use this form to ensure all required information is submitted to the GCP Inspectorate.** If the MHRA template form is not used, the written report should clearly state that it relates to the notification of a serious breach.
- The Sponsor may initially contact the MHRA Inspectorate by telephone to discuss the breach and follow up with a written notification within 7 days of the Sponsor becoming aware of the breach. For current contact details for the Inspectorate, please refer to the MHRA web site.
- Wherever possible, the MHRA will provide an acknowledgement of receipt for notifications.
- It is recommended that the sponsor also informs the relevant Chief Investigator and/or Principal Investigators (as applicable) of the breach notification. Communication in this regard facilitates the implementation of corrective and preventative actions.

### **E. Identifying serious breaches**

Deviations from clinical trial protocols and GCP occur commonly 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 MHRA as a serious breach.



## What needs to be reported?

- Any serious breach of:
  - (a) The conditions and principles of good clinical practice in connection with **that** trial (*as defined in UK legislation*); or
  - (b) The protocol relating to that trial, as amended from time to time in accordance with regulations 22 to 25.
- For the purposes of this regulation, a “serious breach” is a breach which is **likely** to effect to a **significant** degree:
  - - (a) The safety or physical or mental integrity of the subjects of the trial (*this should be relevant to trial subjects in the UK*); or
    - (b) The scientific value of the 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 data to key analysis parameters, the impact of excluding the data from the analysis etc.

It is the responsibility of the Sponsor to assess the impact of the breach on the scientific value of the trial.

This assessment should be documented, as the appropriateness of the decisions taken by the Sponsor may be examined during MHRA inspections. If the Sponsor is unclear about the potential for a breach to have significant impact on the scientific value of the trial, the Sponsor should contact the MHRA to discuss the issue.

See Appendix I for further information relating to expectation for serious breach topics, this may help when deciding on whether to submit a serious breach notification. Appendix II 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.

It is also the responsibility of the Sponsor to take appropriate corrective and preventative actions in response to the serious breach, and to document these actions. Actions may also be taken by the MHRA, as described below.

## What to notify (hints and tips)?

It is strongly recommended that organisations use the provided form to ensure all required information is submitted to the GCP Inspectorate and this should reduce the likelihood of additional information being requested. You **do not have to wait** until you have all the information, **follow-up reports are acceptable**. If the investigation or corrective and preventative action is on-going at the time of reporting the serious breach, it is acceptable to indicate your plans with projected timelines for completion. In such case, you should indicate in the initial report when these are expected to be completed and what follow-up reports will be provided to the Inspectorate and when.



Follow-up reports should be made in writing (the serious breaches form can also be used for this) and should:

- Be clearly identified as a follow-up report.
- Identify the unique GCP identification allocated when your initial report was acknowledged (if you are aware of this information).
- Follow-up reports should include all previously submitted information with new information added in a clear and transparent way. Each report form should be a complete record up to that point and therefore only the latest form is needed for review.
- Be forwarded to the inspector dealing with your initial notification directly or via the mailbox.

## **F. MHRA Actions**

Upon receipt of a serious breach notification, the MHRA will review and assess the notification, and a variety of actions may be taken, depending on the nature of the breach and its potential impact. In general:

1. The GCP Inspectorate checks the serious breach mailbox.
2. Receipt of the notification will be sent and a GCP Inspector will be assigned to review.
3. The Inspector is responsible for reviewing the serious breach.
4. The inspector will decide if:
  - the referral only requires to be logged with no further action (the case may be examined during future MHRA inspections).
  - further information/investigation/CAPA is required. If insufficient information is provided in the initial notification to assess the impact of the breach, follow-up information will be requested.
  - if any other bodies are required to be notified (for example, other competent authorities/EMA, Licensing Division, Clinical Trials Unit (CTU), HRA, Research Ethics Committees, other GxP areas, etc.)
  - further actions are required (for example, a referral to the MHRA Inspection Action Group if the issue is critical or trigger an inspection to investigate further).
  - referral to CTU for consideration of suspension or termination of a clinical trial authorisation.
  - referral to the MHRA Enforcement Unit for consideration of enforcement action, for example, infringement notices, criminal investigation.
  - referral to professional bodies, for example, the General Medical Council.
5. Once any/all required actions have been satisfactorily completed, the inspector will close the referral.

## **G. Organisation Responsibilities**

### **Sponsor:**

There should be a formal process in place to cover the legislative requirements of serious breach notifications. These should include:



- Receipt and assessment (i.e. assessment of deviations/violations by Sponsor/delegate, isolated/systematic incident, patient(s) harmed or put at risk/data credibility etc.)
- Investigation
- Corrective and preventative action (CAPA)
- Reporting to the MHRA
- Compliance with the 7-day reporting timescale.

Lack of systems and failure to report serious breaches may result in findings at GCP Inspections (the grading will depend on the impact of the issue).

#### **Investigator/Institution:**

The investigator/institution (for example, vendor, CRO or investigator site) should also have a process in place to identify and notify the sponsor of serious breaches. This may be a formal SOP or detailed in the protocol or study-specific guidance.

Consideration should be given to what actions to take if the Sponsor does not report the breach to the MHRA (due diligence is required – for example, should you continue with the trial? Should you report to the authorities?)

#### **Retention:**

Where an organisation decides to retain the documentation will depend on each organisation's quality systems. However, as a minimum, a copy should be retained in the relevant Trial Master File/s.

#### **Circulation:**

*Internally:* This will depend on who needs to be informed as per the organisations procedures regarding responsibility for the decision, and notification of the serious breach to the MHRA (for example, clinical, regulatory, QA, management etc.)

*Externally:* This will depend on the nature of the breach and may include other MHRA departments (where legislation may require notifications, for example, CTU, DMRC), regulatory agencies and research ethics committees.

However, it is also important that the breach is circulated/made available to relevant staff for inclusion of relevant information in the clinical study report or publication. Serious breaches relating to investigator sites/laboratories should also be available to those selecting sites for studies, so that an assessment can be made before using non-compliant sites in future studies.

## **H. References**

- **Statutory instrument 2004/1031:** The Medicines for Human Use (Clinical Trials) Regulations 2004.
- **Statutory Instrument 2006/1928:** The Medicines for Human Use (Clinical Trials) Amendment Regulations 2006.
- See also MHRA GCP Guide 2012



## **Appendix I - Expectations for Specific Serious Breach Topics**

### **1. Should proof of fraud relating to clinical trial records or data be reported as a serious breach?**

If the fraud is likely to have a significant impact on the integrity of trial subjects or the scientific value of the data, this will be a serious breach.

Although not a legal requirement under Regulation 29A, the MHRA GCP Inspectorate encourages the reporting of all confirmed instances of clinical trial fraud occurring at sites in the UK, which the Sponsor becomes aware of. The reason for this is that, although fraud at one particular trial site may not have a significant impact on scientific value or subject integrity for that particular trial, the MHRA would wish to assess the impact on other trials or subjects/patients at that site.

If clinical trial fraud is identified at a non-UK trial site, for a trial that is also being conducted in the UK, a serious breach notification should be submitted to MHRA if the fraud is likely to have a significant impact on the integrity of trial subjects in the UK or on the overall scientific value of the trial. A site refers to any site involved in the trial, for example, a CRO or other contracted organisation and not solely to investigator sites (such as laboratories analysing samples from UK patients/subjects).

### **2. Should a breach of GCP or the protocol leading to the death, hospitalisation or permanent disability of a trial subject in the UK be reported as a serious breach?**

Serious Adverse Events (SAEs) and Suspected Unexpected Serious Adverse Reactions (SUSARs) resulting from a breach of the conditions and principles of GCP or a breach of the protocol, will constitute a serious breach. However, it should be noted that not every SAE or SUSAR would routinely be classified as a serious breach.

Also, submission of a serious breach notification to the MHRA Inspectorate does not obviate the requirement for a SUSAR report (where applicable) to be submitted to the concerned competent authorities, for example, via the EudraVigilance database. If the breach also resulted in a temporary /permanent halt to the trial, a substantial amendment would need to be submitted to the MHRA CTU and a further amendment approved to re-start the trial.

### **3. Should a failure to report adverse events, serious adverse events or SUSARs in accordance with the legislation be reported as a serious breach?**

If this failure results in trial subjects, or the public, in the UK being put at significant risk, then this will constitute a serious breach, for example, inadequate safety reporting in dose escalation studies may impact on the decision to escalate to the next dose level.

### **4. Should persistent or systematic non-compliance with GCP or the protocol be reported as a serious breach?**

If this non-compliance has a significant impact on the integrity of trial subjects in the UK or on the scientific value of the trial, this will constitute a serious breach. For example, widespread and uncontrolled use of protocol waivers affecting eligibility criteria, which leads to harm to trial subjects in the UK or which has a significant impact



on the scientific value of the trial. Another example would be an investigator repeatedly failing to reduce or stop the dose of an IMP in response to a trigger defined in the protocol (for example, abnormal laboratory results).

**5. Should a failure to control investigational medicinal product(s) be reported as a serious breach?**

This will constitute a serious breach if the failure results in trial subjects or the public, in the UK being put at significant risk or the scientific value of the trial being compromised. If a serious breach occurs due to an IMP defect, a drug defect report may need to be submitted to the MHRA Defective Medicines Reporting Centre (DMRC), in addition to the serious breach notification.

**6. For trials that are on-going in the UK, should serious breaches that occur at non-UK sites be reported?**

If a serious breach is identified at an investigator site outside the UK that has a significant impact on the integrity of trial subjects at that non-UK site and is likely to have a significant impact on the integrity of trial subjects in the UK, then this will require notification to the MHRA. For example:

- The cause of the breach may be such that the breach may occur at other trial sites, e.g. death of a subject due to incorrect administration of IMP resulting from erroneous reconstitution instructions in the protocol. It should be noted that as well as having to notify the MHRA of the serious breach, other concerned competent authorities may also need to be informed.
- In relation to the example above, an urgent safety measure (USM) may need to be implemented to address the cause of the breach. If, in order to address the cause of a serious breach, an USM is implemented at UK sites, to amend the conduct of the trial or suspend the trial, the USM notification should be sent by the Sponsor to the MHRA Clinical Trials Unit within 3 days of identifying the measures to be taken (in accordance with Regulation 30), in addition to the serious breach notification to the MHRA Inspectorate.
- If a serious breach is identified at an investigator site outside the UK, which is likely to affect to a significant degree the overall scientific value of the trial and the result will impact on UK patients or the UK public (for example, data will be used in a marketing authorisation application that affects the UK), then this breach should be notified to the MHRA (other concerned competent authorities may also need to be informed).



**Appendix II Examples of Serious Breaches Notified to MHRA (this is not an exhaustive list)**

Notifier	Details of Breach Reported	Is this a Serious Breach?
Sponsor	<p>Dosing errors reported:</p> <p><b>1)</b> A subject was dosed with the incorrect IMP, which was administered via the incorrect route (the IMP used was from a completely different clinical trial to the one the subject was recruited to).</p> <p><b>2)</b> 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.</p> <p><b>3)</b> One subject was administered 6 additional doses of IMP. The subject was to receive IMP on day 1 and 8 but instead received IMP on days 1 to 8. The subject experienced a severe adverse event as a result.</p> <p><b>4)</b> A subject took IMP that had expired two days ago. The subject did not experience any adverse events and this issue was not likely to affect the data credibility of the trial.</p>	<p><b>Yes</b>, there was significant potential to impact the safety or physical or mental integrity of trial subjects.</p> <p><b>Yes</b>,</p> <ul style="list-style-type: none"> <li>• there was impact on the safety or physical or mental integrity of trial subjects or on the scientific value of the trial</li> <li>• this issue was systematic and persistent leading to a constant breach of the conditions and principles of GCP in connection with that trial or the trial protocol</li> <li>• this issue persisted despite the implementation of a corrective and preventative action plan.</li> </ul> <p><b>Yes</b>, there was impact on the safety or physical or mental integrity of trial subjects and on the scientific value of the trial</p> <p><b>No</b>, 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.</p>
Sponsor	IMP temperature excursions reported.	<b>Yes</b> , if the situation was not managed and subjects were dosed

		<p>with IMP assessed as unstable, which resulted in harm/potential to harm subjects.</p> <p><b>No</b>, 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.</p>
Sponsor	Multiple issues with the Interactive Response Technology (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.	<b>Yes</b> , there was impact on the safety or physical or mental integrity of trial subjects and this issue persisted leading to a constant breach of the conditions and principles of GCP in connection with that trial or the trial protocol, despite the implementation of a corrective and preventative action plan.
Sponsor	On two separate occasions the Sponsors identified issues with the same organisation. First with consenting and then with potential 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.	<b>Yes</b> , this subsequently led to enforcement action against the organisation in question.
Sponsor	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. 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 sent to MHRA confirmed the Sponsor concerns over consenting and data changes made to source without an adequate written explanation.	<b>Yes</b> <i>Note: not all of the information was provided in the original notification, the Sponsor provided follow-up updates.</i>
Sponsor	A clinical trial subject attended A&E who attempted to contact the pharmacy department (using the phone number listed on the emergency card issued to the subject) in order to break the unblinding code. Pharmacy were 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	<b>Yes</b> , as this had significant potential to harm the subject if unblinding would have affected the course of treatment.

	emergency situation.	
CRO	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 amendment was required to recruit more subjects to meet the endpoint. Subjects were dosed unnecessarily as a result of this error.	<b>Yes</b>
CRO	Subject safety was compromised because repeat ECGs were not performed, as required by the protocol. Also, there was inadequate QC of the interim safety reports used for dose escalation which has potential for stopping criteria to be missed.	<b>Yes</b>
Contractor	The Investigator failed to report a single SAE as defined in the protocol (re-training provided).	<b>No</b> , 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.
Identified during inspection	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. Subjects were exposed to an increased risk of thrombosis.	<b>Yes</b>
Identified during inspection	A potential serious breach was identified, but not reported (documentation in the Sponsor's TMF identified that there may have been fraud at an investigator site, re-use of previous time point data in later time points). The Sponsor had investigated and the issue was subsequently found to be a genuine error and not fraud.	<b>No</b> , on this occasion.  <i>However, had this been identified as fraud impacting on the integrity of the data, then this serious breach would not have been notified within the regulatory timeframe (i.e. 7 day window).</i>
Sponsor	Patient Information Leaflet and Informed Consent updated, but at one trial site this was not relayed to the patients until approximately	<b>No</b> , if this was not a systematic or persistent problem and if no harm to trial subjects resulted from the delay.

	2-3 months after approval. <i>More information on the potential consequences of the delay should have been provided.</i>	<b>Yes</b> , 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).
Sponsor	Visit date deviation. <i>A common deviation in clinical trials.</i>	<b>No</b> , a minor protocol deviation, which does not meet the criteria for notification.
MHRA (CTU)	The GCP Inspectorate was notified that a substantial amendment had been submitted regarding changes to dosing on a first in human study, as a result of an SAE after dosing the initial subject. The sponsor had temporarily halted the trial and only after further investigation had assigned the SAE as unrelated. The sponsor had <b>not</b> notified the CTU of the “urgent safety measure” implemented or reported the SAE as a potential SUSAR.	<b>Yes</b>
NRES	The early destruction of investigator site files (i.e. one study had only been completed a year earlier and one study was still ongoing).	<b>Yes</b>
Member of public	A member of public received a named invite to be a volunteer in a clinical trial (no specific trial mentioned). However, this person was not on the organisation’s volunteer database and had not participated previously in a study. On further investigation by MHRA, it was revealed that the organisation had contracted the use of a mail shot organisation to send a generic mail shot to a list of people in a specific location, over a certain age. This had been approved by the REC.	<b>No</b>