Guideline for management and reporting of serious breaches_ Sites

HOVON Breach coordinators:	hovonbreaches@erasmusmc.nl
Jeannine Refos	Senior Global Clinical Project Manager (CPM)
Marlies Groenendijk	Pharmacovigilance coordinator (PV coordinator)
Romy Lussenburg	Senior Pharmacovigilance officer (Senior PV officer)

This document provides instructions, guidelines and background information regarding the Breach Database using the Electronic Data Capture (EDC) system of ALEA, as implemented by HOVON.

Table of Contents

1. Glossary

Affected Member State (AMS)	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.
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)	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.
CTIS	Clinical Trials information System.
Protocol deviation	Protocol deviation or violation is any non-compliance from the study procedures or treatment plans as specified in the IRB-approved protocol.
Sponsor	An individual, organization or group which has taken on responsibility for securing the arrangements to initiate manage and finance study.
Suspected serious breach	A deviation that is judged by the reporter as a possible serious breach but has yet to be formally confirmed as a serious breach by the sponsor.
Serious breach (SB)	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.
Reporter	Reports the breach (Site PI or other authorized site staff, authorized HOVON personnel)
HOVON breach coordinator	HOVON Breach coordinators, will assess any reported breach.
ALEA study BREACHES	HOVON Breach database/eCRF developed for the reporting of all (suspected) serious breaches in the HOVON ALEA database.
Breach Report number	This is a unique number generated by ALEA for every reported breach. (HOVON_ BR (=Breach)_year_number X)

2. Introduction and Scope

As of January 31, 2022, the regulation (EU) No. 536/2014 (Clinical Trial Regulation, CTR) applies for conducting clinical trials with drugs.

Under this regulation the sponsor has a primary responsibility for determining whether any suspected breach meets the definition of a **serious breach** in a clinical trial.

This is defined by Regulation (EU) No 536/2014, 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.

3. Actions to report serious breaches

Any suspected serious breach must be reported as soon as possible to HOVON via the ALEA BREACH database (eCRF) or via the paper CRF:

A. Complete a report of the suspected breach in ***ALEA study BREACHES.***

or

B. Send a completed breach paper CRF (see appendix A) to hovonbreaches@erasmusmc.nl

3.1 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

That is likely to affect to a significant degree:

1. The safety of a trial participant.

and/or

2. The rights of a trial participant.

and/or

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

3.2 Reporting steps of a suspected serious breach:

After becoming aware of a suspected serious breach, the breach must be reported to HOVON as soon as possible.

- Reporter: from becoming aware of a (suspected) serious breach, assesses and investigates in a timely manner if the breach may have a significant impact on **safety or rights of participants** and/or **the reliability and robustness of the data.**
- Reporter: makes every effort to substantiate that the breach is a (suspected) serious breach.
- Reporter: does not wait to obtain all of the details related to the breach prior to the notification of HOVON.
- Reporter: (if applicable) informs the site PI of the possible breach and (if applicable) inquires more information from patient physician /local lab/local pharmacy.
- Reporter: provides updates to HOVON whenever further information becomes available.
- HOVON has the primary responsibility for determining whether any suspected breach meets the definition of a serious breach..

3.3 Timelines for HOVON to report a serious breach in CTIS

On reasonable grounds based on evidence to believe that a serious breach has occurred, **HOVON** must report the serious breach via the secure module of the Trials information System (CTIS) within **7 calendar days** after becoming aware of the serious breach.

Once submitted 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.

Note:

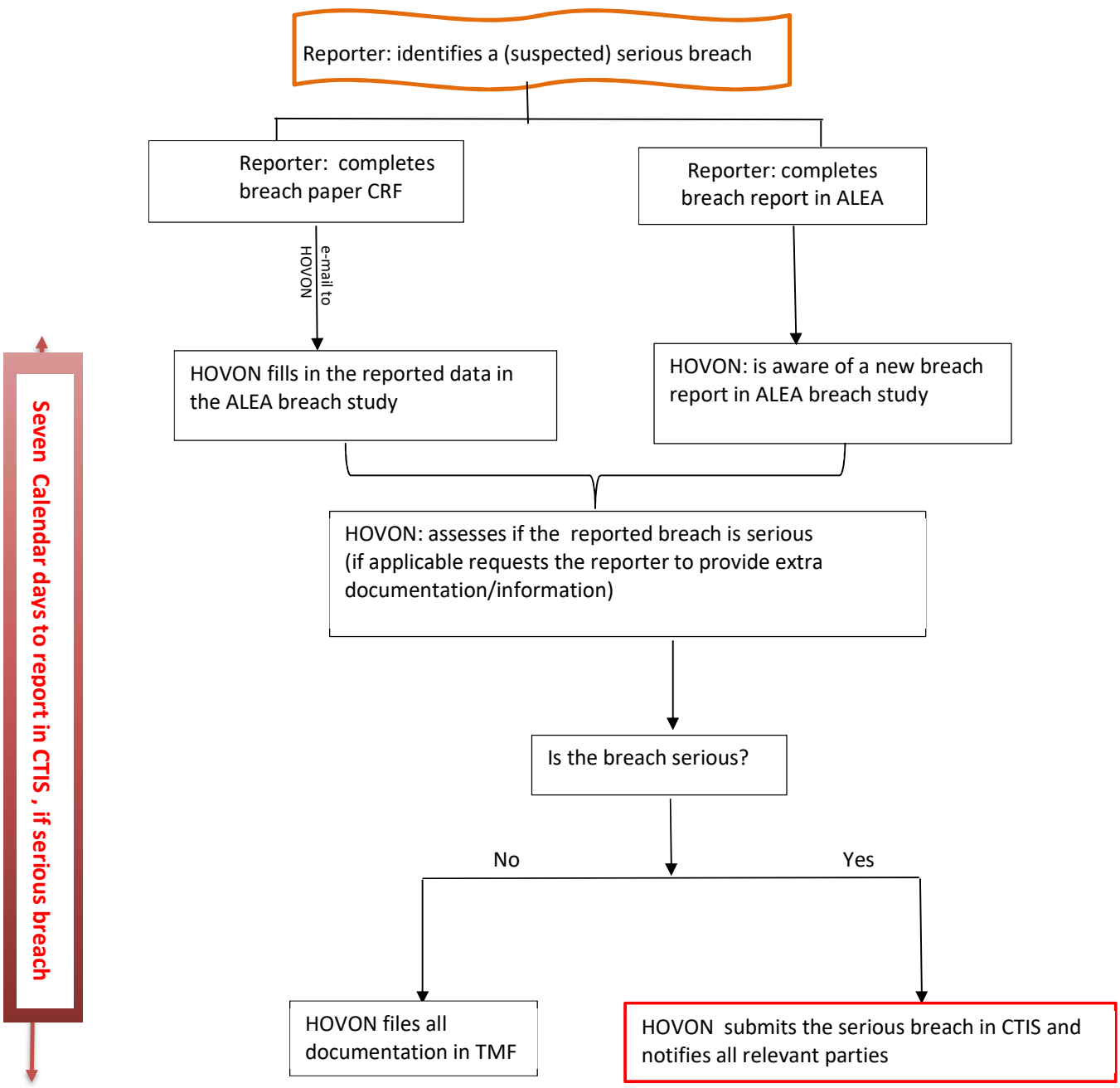
- If HOVON determines that the reported (suspected) serious breach is not serious, no breach will be reported in CTIS. Only breaches hat have been assessed as serious by HOVON are reported.

- For serious breaches occurring at a trial site, HOVON will notify all relevant partners that a serious breach has occurred.

- If HOVON determines that the reported (potential/suspected) serious breach is serious, HOVON will ensure the reporting of the serious breach to the member states concerned authorities no later than 7 days of becoming aware of that breach.

- If HOVON determines that the reported (potential/suspected) serious breach is not serious, HOVON will file the documentation in the TMF.

4. Flowchart actions to report a (suspected) serious breach



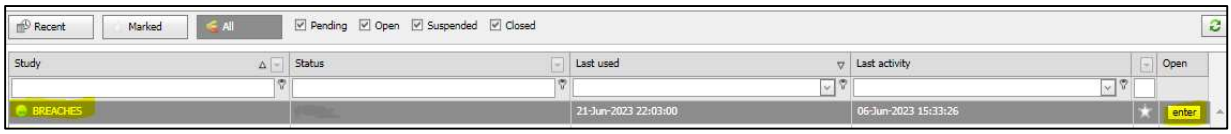
5. ALEA Breach study; ALEA instructions

This chapter contains instructions on how to report the suspected serious breach data in the ALEA study BREACHES database

5.1 Log in in ALEA to register a (potential) serious breach

1. Log in via the URL https://aleaclinical.com/Hovon/DM/DELogin.aspx.
If you have access to multiple studies, you will enter a Study Selection page upon login.

2. Select/Enter the study BREACHES



3. To register a NEW (potential) breach select ''Add new breach''

5.2 Breach registration

Once the form for a new breach is opened, a breach report number (unique breach number) and the initiation date (current date) will be automatically filled in.

1. Submit the form.

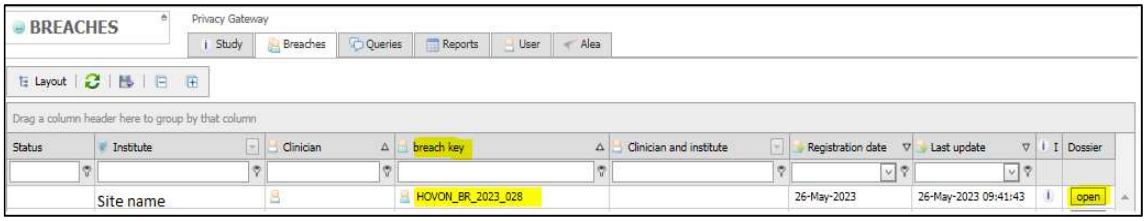
*breach report number and date are examples
* breach report number = HOVON_ BR (=Breach)_year_number X

2. After you have submit the new breach registration form. You will be returned to the ''home'' study BREACHES page.
3. The initiated breach report still needs to be completed. Refer to paragraph 5.3

5.3 Complete the breach report

The initiated breach report still needs to be completed.

1.Select/ open your breach number to continue with the report.



2. Open de Breach report

3. Complete the report. All red fields are mandatory!

- **For the full report please refer to appendix A HOVON breach paper CRF and/or ALEA database; study BREACHES**
- **<u>After completing the report. Please save the data, and submit the breach report form.</u>**

6. Reference

Guideline for management and reporting of serious breaches of regulation (EU) no 536/2014; 13 December 2021

1. APPENDIX A: HOVON Breach paper CRF - attached as a separate document

2. APPENDIX B: Examples of serious breaches -- attached as a separate document

Note: Please refer to the most recent *Guideline for the notification of serious breaches of Regulation (EU) No 536/2014 or the clinical trial protocol*

BREACH REPORT

Please note that this form has to be completed and submitted in ALEA.
More information about the submission of the Breaches eCRF in ALEA can be found in the instruction manual.
In case of (other) questions, contact the Breach coordinators at hovonbreaches@erasmusmc.nl

New or updated Breaches that cannot be entered digitally can also be sent to the Breach coordinators via hovonbreaches@erasmusmc.nl.
In the last case, please use this form to report all breaches as described in the trial protocol and manual.
An **initial report** must be submitted / sent to HOVON as soon as becoming aware of the breach.

0. SPONSOR INTERNAL IDENTIFICATION AND INFORMATION ON BREACH REPORT		
0.4	Who identified the breach?	☐ Local datamanagement ☐ Site Staff ☐ Monitor ☐ Other
0.5	Breach type	☐ Protocol ☐ Regulation (EXTR, GxP, GDPR or other) ☐ Quality Management System ☐ Other breach/incident/issue
0.6	Immediate action taken?	☐ No, please specify at 0.6.0 ☐ Yes, please specify at 0.6.1 ☐ Not applicable, please specify at 0.6.2
0.6.0	*Explain why no immediate action was taken*	
0.6.1	*Describe which immediate action was taken (what, by who, date, time, etc.)*	
0.6.2	*Explain why immediate action was not applicable*	

BREACH REPORT

A. GENERAL INFORMATION		
A.0.0	Date of becoming aware of the breach	
A.0.1	Was the date of becoming aware of the breach the same as the date of the breach?	☐ Yes ☐ No
A.0.2	Date of breach	
A.2	Involved HOVON trial	
A.5	Are other clinical trials impacted by the same breach?	☐ No ☐ Not Known ☐ Yes
A.5.1	Involved other (HOVON) trial name	
A.5.3	Specify EU CTR number *(if it does not concern a HOVON trial)*	
A.6	Details of the site where the breach occurred	
A.6.0.1	Country	
A.6.0.2	City	
A.6.0.3	Site name	
A.6.1	Tel. no. site	
A.6.2	E-mail site	
A.6.3	Involved patient(s) *(Please fill out Patient Study ID if applicable)*	

BREACH REPORT

B. DETAILS OF THE BREACH		
B.1	Brief description of the breach	
B.2	(Potential) impact of the breach	
B.2.1	Safety of the trial Participant?	
B.2.1.1	Category of impact	☐ IMP ☐ IRT issues ☐ Source data ☐ Sample processing ☐ SAE reporting ☐ Access to data ☐ DSMB/DMC ☐ Other ☐ Temperature monitoring ☐ Potential fraude ☐ Emergency unblinding ☐ Protocol compliance ☐ Consent ☐ Randomization/stratification errors ☐ Privacy
B.2.1.2	Description of the impact	
B.2.2	Rights of the trial Participant?	
B.2.2.1	Category of impact	☐ IMP ☐ IRT issues ☐ Source data ☐ Sample processing ☐ SAE reporting ☐ Access to data ☐ DSMB/DMC ☐ Other ☐ Temperature monitoring ☐ Potential fraude ☐ Emergency unblinding ☐ Protocol compliance ☐ Consent ☐ Randomization/stratification errors ☐ Privacy
B.2.2.2	Description of the impact	

BREACH REPORT

B.2.3	Data reliability & robustness?	
B.2.3.1	Category of impact	☐ IMP ☐ Temperature monitoring ☐ IRT issues ☐ Potential fraude ☐ Source data ☐ Emergency unblinding ☐ Sample processing ☐ Protocol compliance ☐ SAE reporting ☐ Consent ☐ Access to data ☐ Randomization/stratification errors ☐ DSMB/DMC ☐ Privacy ☐ Other
B.2.3.2	Description of the impact	
B.2.4	Regulatory?	
B.2.4.1	Category of impact	☐ IMP ☐ Temperature monitoring ☐ IRT issues ☐ Potential fraude ☐ Source data ☐ Emergency unblinding ☐ Sample processing ☐ Protocol compliance ☐ SAE reporting ☐ Consent ☐ Access to data ☐ Randomization/stratification errors ☐ DSMB/DMC ☐ Privacy ☐ Other
B.2.4.2	Description of the impact	
B.2.5	Other (HOVON trials)?	
B.2.5.1	Category of impact	☐ IMP ☐ Temperature monitoring ☐ IRT issues ☐ Potential fraude ☐ Source data ☐ Emergency unblinding ☐ Sample processing ☐ Protocol compliance ☐ SAE reporting ☐ Consent ☐ Access to data ☐ Randomization/stratification errors ☐ DSMB/DMC ☐ Privacy ☐ Other
B.2.5.2	Description of the impact	
B.3	Other relevant details / information	

Appendix B – Examples of serious breaches

Reference: Guideline for the notification of serious breaches of Regulation (EU) No 536/2014 or the clinical trial protocol EMA/698382/2021) 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.