STANDARD OPERATING PROCEDURE FOR REPORTING BREACHES IN CLINICAL RESEARCH

SOP NUMBER:	TASC SOP059 v6
AUTHOR:	Patricia Burns
EFFECTIVE DATE:	28 Oct 2024
REVIEW DATE:	28 Oct 2026

1. PURPOSE

This Standard Operating Procedure (SOP) describes recording and reporting breaches in interventional studies sponsored and/or co-sponsored by the University of Dundee and/or NHS Tayside.

This includes Clinical Trials of Investigational Medicinal Product (CTIMP) and any other projects deemed by Sponsor to be 'interventional'.

It describes both the role of the research personnel in identifying and notifying Sponsor of the breach and the role of Sponsor and their appropriate management of the breach.

2. SCOPE

This SOP applies to all researchers and Sponsor staff participating in interventional research projects sponsored or co-sponsored by University of Dundee and/or NHS Tayside.

3. RESPONSIBILITIES

Chief Investigator (CI):	Reporting breaches to Sponsor and Research Ethics Committee (REC) if a condition of ethical favourable opinion. Reporting any breaches to the funder if it is a condition of the agreement. Implementing any Urgent Safety Measures.
Principal Investigator (PI):	Reporting Breaches to CI or delegate.
Sponsor:	Report Serious Breaches in CTIMP/device studies to Medicines and Healthcare Products Regulatory Agency (MHRA) and REC.
Data Management:	Reporting to Sponsor of any data indicative of fraud.
Senior Research Governance Manager/Delegate:	Liaising with MHRA and/or REC on behalf of Sponsor.

Notifying the Serious Breach Review Group (SBRG) and CI when breach is closed.

Research Governance Manager:

Liaising with REC and CI on behalf of Sponsor for non-CTIMPs.
Escalating breaches and areas of concern to Senior Research Governance and to SBRG.
Notifying the CI when breach is closed.

Note: anybody can report breaches, including breaches of General Data Protection Regulations (GDPR).

4. PROCEDURE

4.1 Definitions

There is no definitive guidance regarding the meaning of the term deviation (or violation) and therefore it is not used in this document.

Any departure from:

- the Protocol
- the principles of Good Clinical Practice (GCP)
- Written procedures (such as SOPs)
- Regulatory requirements
- Confidentiality and Data Protection

may be referred to as deviations. All deviations are breaches.

4.2 Key Timing

- All breaches must be reported to the Sponsor without delay.
- The CI must ensure that potentially Serious Breaches in CTIMPs of the protocol and/or the principles of GCP are reported to the Sponsor within 24 hours of being identified.
- In a multi-site project, the PI of a CTIMP must report potentially serious breaches to the CI who must notify Sponsor within 24 hours of this notification.
- The CI must assess a breach as soon as it is identified and make an initial assessment as to whether the Breach is Serious or non-serious.
- The Sponsor must report Serious Breaches in CTIMPs to the MHRA within 7 calendar days of the Breach being notified to Sponsor.
- For all research projects, the Sponsor is responsible for reporting Serious Breaches to the relevant REC within 7 calendar days of the breach being confirmed as serious.
- Potential breaches of GDPR must be reported to the Data Protection Officer.

All Breaches must be recorded on a Breach Report Log (Doc Ref 006) retained in the Trial Master File (TMF).

The Breach Reporting & Corrective Action/Preventative Action (CAPA) Form (Doc Ref 064) must be completed by the CI or delegate and include:

- An overview of the incident and its cause.
- Detail of any CAPA.
- An assessment of the likelihood of a recurrence.
- An impact assessment on any work performed prior to the event, which may be compromised.
- Outline of any changes which may be required to the protocol.
- Likely timeline for CAPA and amendment approval (if applicable).

This must be sent to TASCpotentialbreach@dundee.ac.uk and is to be acknowledged by return.

4.3 Sponsor breach assessment and further investigation of breach

CTIMPs - the Senior Research Governance Manager (SRGM) shall make the initial assessment of seriousness and in liaison with the Quality Assurance Manager (QAM) review the proposed CAPA.

Non-CTIMPS - the Research Governance Manager (RGM) shall make the initial assessment of seriousness and if required liaise in liaison with the SGRM and QAM, review the proposed CAPA.

The decision may be taken to classify the breach as:

- Potential Serious Breach
- Potential breach of GDPR
- Non serious breach
- Not a breach.

For potential serious breaches, a SBRG will be assembled to facilitate a systematic evaluation of the issue. A face-to-face SBRG meeting may be convened by the SRGM or delegate, comprising of the CI or PI, lead physicians for the Sponsor(s), key members of the research team (e.g. Trial Manager) and other members as appropriate.
The SBRG meeting may also involve experts from within the Sponsor organisation(s) or external parties as required. Where deemed appropriate, this meeting may take place by telephone or be conducted by a series of emails.

The assessment made by SBRG shall:

- Identify what exactly has been breached.
- Identify how the breach impacts on trial participants and/or the scientific integrity of the research.
- Whether to implement urgent safety measures, such as stopping the research project or specific aspects of the project immediately, pending any further investigation as necessary.
- Confirm whether the breach is a Serious Breach or not.
- Address any systematic failure and upgrade a non-serious to Serious Breach.

- Whether the proposed CAPA is appropriate and timelines suitable.
- Require further CAPA is required - including Substantial Amendment.
- Suspend the project until all necessary corrections and CAPA have been implemented.

Note: a non-serious breach may be upgraded by the SRGM to potentially serious and escalated to SBRG, if deemed part of a systematic failing.

4.4 Classifications and CAPA

- A Serious Breach is likely to affect, or have the potential to affect, to a significant degree: the safety, physical or mental integrity of research participants, and/or the scientific value of the research. Serious Breaches must be reported to the MHRA and REC that gave favourable opinion to the project within 7 days of notification to the Sponsor.

- A breach of GDPR is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. Data breaches may involve Personal Health Information, Personal Identifiable Data (PID), trade secrets or intellectual property.
  These breaches must be notified on to the Data Protection Officer and/or Information Governance Officers of the University of Dundee and/or NHS Tayside.

- A Non-Serious Breach has no impact on a participant's safety or wellbeing, and/or the scientific integrity of the research.

- Not a breach- if classified as not a breach, no further action will be required by the Sponsor.

4.5 Notification of a Serious Breach to the MHRA

4.5.1 The SRGM or Sponsor delegate will collate all available information to support the decision on classification and complete the notification form to MHRA available on their website.

4.5.2 Prior to submission to MHRA, the SRGM will circulate the MHRA Form to the SBRG to agree the decision. Where consensus cannot be reached, the NHS Tayside R&D Director's decision is final.

4.5.3 The report must be submitted to the MHRA within 7 days of the Sponsor first becoming aware that the breach is serious.

4.5.4 The MHRA Form must be sent to the relevant REC and the CI for the TMF and filed in the Sponsor File.

4.6 Follow up of Breach CAPA plan

- Depending on the initial assessment of seriousness and impact, an audit of the study, its management systems and procedures may be performed.
- If the CAPA is not progressing according to agreed timelines, the SRGM/ QAM or delegate will inform the SBRG for further action.
- When all corrective actions required have been addressed, the closed Breach Report will be filed in the Sponsor File and TMF.
- If the trial has been temporarily halted, the CI will be advised of when the trial may re-commence.

4.7 Data Breach – receipt of Personal Identifiable Information (PID)

- Individuals or teams who receive PID that they would not normally have access to are **not** in breach of GDPR.
- The breach is by the individual who sent the PID.
- Under no circumstances should the PID be forwarded on.
    - This **would** constitute a breach of GDPR and must be notified as per this SOP.

4.7.1 PID received by email

- The information must be deleted and purged from the email system.
- The person responsible for sending the PID and breaching GDPR must be notified immediately of the breach and advised that they should notify their own Data Protection Officer.
- The person responsible must also be told of the actions taken by the individual in receipt of the data; that the data was not forwarded on and has been deleted and purged.

4.7.2 PID received as hard copy

- This must be stored securely, in a locked filing cabinet, and contact made with the sender/site to establish if this must be returned to the site or can destroyed.
- The action must be documented.

Any suspected data breach involving University of Dundee must be reported by the recipient to dataprotection@dundee.ac.uk or x84441 immediately.

Any suspected data breach involving NHS Tayside must be reported by the recipient to tay.informationgovernance@nhs.scot immediately.

5. ABBREVIATIONS & DEFINITIONS

CAPA	Corrective Action/Preventative Action
CI	Chief Investigator
CTIMP	Clinical Trial of Investigational Medicinal Product

GCP	Good Clinical Practice
GDPR	General Data Protection Regulations
MHRA	Medicines and Healthcare Products Regulatory Agency
PI	Principal Investigator
PID	Personal Identifiable Data
QAM	Quality Assurance Manager
REC	Research Ethics Committee
RGM	Research Governance Manager
SRGM	Senior Research Governance Manager
SBRG	Serious Breach Review Group
SOP	Standard Operating Procedure
SRGM	Senior Research Governance Manager
TASC	Tayside Medical Science Centre
TMF	Trial Master File

6. ASSOCIATED DOCUMENTS & REFERENCES

Doc Ref 006: TASC Breach Report Log
Doc Ref 064: TASC Breach Reporting & CAPA Form

7. DOCUMENT HISTORY

History prior to 2021 is in the archived SOPs available from TASC Quality Assurance Dept.

Version Number:	Reviewed By (Job Title):	Effective Date:	Details of editions made:
5	Patricia Burns (Senior Research Governance Manager)	28/10/2022	No changes required at this scheduled review.
6	Patricia Burns (Senior Research Governance Manager)	28/10/2024	No changes required at this scheduled review.

8. APPROVALS

Approved by:	Date:
Dr Valerie Godfrey, TASC Quality Assurance Manager, on behalf of TASC Clinical Research Guidelines Committee	25 Oct 2024