STANDARD OPERATING PROCEDURE 36
Warwick Clinical Trials Unit (WCTU) Data Breach Incident Management Procedure

Version:	**4.0**	Effective Date:	11 July 2024
Issue Date:	27 June 2024	Review Date:	11 July 2026
Author:	Jill Wood, Quality Assurance (QA) Manager, WCTU		
WCTU Reviewers:	Susie Hennings, Senior Project Manager, WCTU Sara Wood, Clinical Trials Manager, WCTU Loraine Chowdhury, Clinical Trials Coordinator, WCTU Kerry Raynes, Clinical Trial Manager, WCTU Claire Jacques, Clinical Trial Manager, WCTU		
Sponsor Reviewers:	Mathew Gane, Research Governance & QA Manager, Research & Impact Services (R&IS)		
WCTU approval:	Natalie Strickland, Head of Operations, WCTU		
Sponsor approval:	Carole Harris, Assistant Director, R&IS (Systems & Strategic Projects) & Head of Research Governance		
Review Lead:	WCTU QA Team		

Contents

Revision Chronology:	**Effective date:**	**Reason for change:**
Version 4.0	11 July 2024	Biennial review: Addition of summary flow chart, multiple clarifications to text and flow. Change to insurance reporting requirements to only immediately notify in the event of a reportable breach
Version 3.0	23 Jun 2022	Urgent addition to accommodate change of guidance around reporting breaches from UoW Processors.
Version 2.0	15 Mar 2022	Updates ahead of biennial review to ensure alignment with the University's breach reporting processes and WCTU non-compliance procedures.
Version 1.1	10 Sept 2020	Removal of DPO name. Generic contact details retained.
Version 1.0	25 July 2019	New document

STANDARD OPERATING PROCEDURE 36
Warwick Clinical Trials Unit (WCTU) Data Breach Incident Management Procedure

1. Purpose and Scope

The purpose of this Standard Operating Procedure (SOP) is to detail procedures to follow for all WCTU staff who process personal identifiable data when there has been a suspected or actual breach of personal identifiable information. This procedure is designed to define WCTU specific processes and should not replace the University's central breach reporting procedure.

This process applies to both data breaches and processor data breaches where the University of Warwick are the Data Controller or Joint Data Controller. Where the University of Warwick (UoW) is not a Data Controller the breach reporting procedures of the controller organisation should be consulted.

The University's Information Management Policy Framework includes policies, guidance and procedures that cover the prevention of personal data breaches from occurring in the first instance. The University policies and procedures can be accessed here: https://warwick.ac.uk/services/idg/it-compliance/policies/ and should be read in conjunction with university research SOPs.

If a personal data breach relates to a research study participant, it is likely to also satisfy the criteria of a study non-compliance and should be recorded as a data breach or processor data breach on the non-compliance log as appropriate. More information on how to manage and record non-compliance is outlined in SOP 31 'Handling non-compliances, research misconduct and serious breaches of GCP and/or Study Protocol'.

2. Definitions

Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal identifiable data transmitted, stored or otherwise processed.
Processor data breach	A personal data breach (as defined above) that originates from a data processor whilst acting under the instruction of the Data Controller. *n.b. all study processors should be detailed on the study Data Flow Map*
Personal Identifiable Data (PID)	Any information relating to an identified or identifiable natural person *('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Incident management	The procedures for supporting the detection, analysis and follow up response in the event of a breach, alerting all relevant parties as soon as possible and resolving the incident in a considered and responsible way to minimise impact.
Data subject	The identified or identifiable living individual to whom personal identifiable data relates.

Data controller	Controllers are the main decision-makers who exercise overall control over the purposes and means of the personal data processing. If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers.
Data processor	Processors act on behalf of, and only on the instruction of the relevant controller.

**A natural person is 'alive' and not deceased. Once a person is deceased, their data is no longer considered personal, however, these data are considered to be confidential, so the Common Law Duty of Confidentiality still applies. Breaches of confidentiality can be reported but there is no legal requirement under UK GDPR.*

3. Background

Data breaches are a very real risk to all organisations that process data, whether a result of human error, equipment failure or criminal activity. Staff involved in running research studies often have access to sensitive personal information, and they are all responsible for ensuring that this information is not disclosed to anyone outside the research team.

The UK General Data Protection Regulation (UK GDPR) introduces a duty on all organisations to notify certain types of personal data breach to the Information Commissioners Office (ICO). Reporting is only required in some circumstances, but the UK GDPR states that organisations must keep records of any personal data breaches, regardless of whether notification is required.

The rapid identification and reporting of personal data breaches is critical to ensuring they are effectively managed and mitigated, and that the University complies with the obligations of the UK GDPR.

4. Procedure

4.1 Responsibilities

University of Warwick Data Protection Officer (DPO) - ***or delegate from the Legal and Compliance Team***	• Overall responsibility for the management of the incidents • Decision whether an incident constitutes a breach • Decision as to whether a breach is reportable to the ICO • Decision on whether it is appropriate to contact the data subject.
All WCTU staff that have access to or process personal data	• Responsible for reporting any personal data breach or processor data breach to the DPO via the University data breach process and for assisting with investigations where necessary.
Head of Operations, QA Managers and Programming Team Manager	• Incident management involving WCTU • To convene as a response team for investigation of reportable personal data breaches
QA Team	• To produce regular oversight reports to both Governance Committee and Sponsorship and Oversight Committee regarding data breaches.

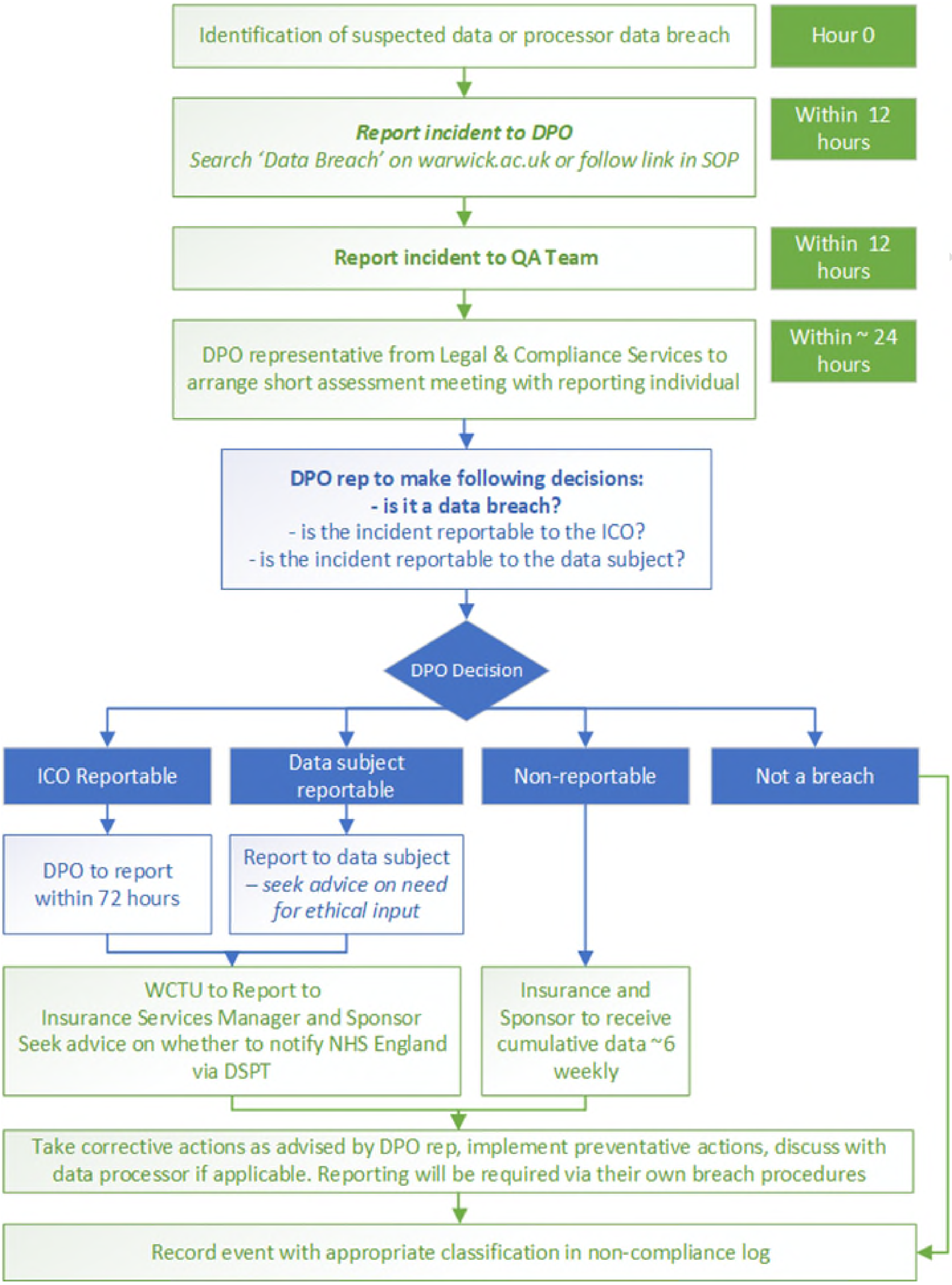
In the case of a processor data breach, the DPO relevant to that site may be responsible for breach investigation and reporting. Where this is the case, it remains our responsibility to notify the site that we believe there to be a breach and that the team involved should also follow their internal data breach procedures.

4.2 When?

All personal data breaches or suspected data breaches identified by staff should be reported to the DPO and the WCTU QA team as a matter of urgency, and within 12 hours of becoming aware of the incident.

It is very important to not delay and to contact the QA team and the Legal and Compliance team promptly even if the incident is only suspected. UK GDPR places a duty on organisations to report certain types of personal data breach to the Information Commissioner's Office within **72 hours of becoming aware of the breach**. This process will be coordinated by the DPO and the Legal and Compliance Team. The QA team can support the process as needed.

4.3 How?


Identification of suspected data or processor data breach
Hour 0
Report incident to DPO
Search 'Data Breach' on warwick.ac.uk or follow link in SOP
Within 12 hours
Report incident to QA Team
Within 12 hours
DPO representative from Legal & Compliance Services to arrange short assessment meeting with reporting individual
Within ~ 24 hours
DPO rep to make following decisions:
- is it a data breach?
- is the incident reportable to the ICO?
- is the incident reportable to the data subject?
DPO Decision
ICO Reportable
Data subject reportable
Non-reportable
Not a breach
DPO to report within 72 hours
Report to data subject – seek advice on need for ethical input
WCTU to Report to Insurance Services Manager and Sponsor Seek advice on whether to notify NHS England via DSPT
Insurance and Sponsor to receive cumulative data ~6 weekly
Take corrective actions as advised by DPO rep, implement preventative actions, discuss with data processor if applicable. Reporting will be required via their own breach procedures
Record event with appropriate classification in non-compliance log

4.3.1 Identification of a suspected data or processor data breach

A personal data breach from a controller or a processor may involve one or more of the following:

- Loss or theft of data or equipment on which data is stored
- Disclosure of information to a third-party organisation which is not authorised to see the data or is outside of the data subject's expectations
- Unauthorised access to confidential or highly confidential University data
- Equipment or system failure, where it normally functions to protect data such as encryption or redaction
- Human error
- Natural phenomena, such as a fire or flood
  Malicious action, such as where information is obtained by deceit or hacking.

4.3.2 Reporting the suspected breach

A suspected personal data breach or suspected processor data breach must be reported to the University **DPO** and the **WCTU QA Team** within **12 hours** of becoming aware.

How to report to the DPO:

- Search 'data breach' at warwick.ac.uk **or**
- Direct link to reporting page: https://warwick.ac.uk/services/legalandcomplianceservices/dataprotection/breaches

4.3.3 Assessment of suspected breach

A representative of the DPO from the Legal and Compliance Team will organise a short assessment meeting with the person reporting the suspected breach. Support and input can be provided by the QA team if needed. During the meeting the representative will decide whether the suspected breach:

- Meets the definition of a data breach or processor data breach
- Is of sufficient risk that it needs reporting to the ICO
- If it requires notification to the data subject

The Legal and Compliance Team may also input on relevant corrective and preventative actions. A summary of the assessment meeting will be generated and returned via email to the reporter. These should be retained in the TMF and ideally signposted to in any non-compliance report.

4.3.4 Other parties where reporting might be required

Depending on the outcome of the DPO decision one or more of the following parties may need to be notified:

4.3.4.1 Notification to the ICO

The University is required to notify the ICO as soon as possible and, where feasible, not later than 72 hours after having become aware, of any personal data breaches involving a high risk to the rights and interests of the affected individuals as per the assessment in 4.3.3. The DPO will make the decision as to whether this should be reported to the ICO. Breaches not involving a high risk are not required to be reported to the ICO by the DPO. It is therefore important that any potential breaches are reported as quickly as possible to the DPO so that Warwick remains compliant with the regulatory breach reporting requirements.

4.3.4.2 Notification to the data subject

Where the personal data breach, or suspected personal data breach, is likely to result in impacting the rights and freedoms of the data subject, action must be taken to ensure that any affected individuals or third parties are notified without undue delay. The data subject should only be notified if the DPO's representative gives authorisation to do so. They should be involved in the content of the notification and consideration should be given to whether this needs ethical input as a patient facing document.

4.3.4.3 Notification to NHS England

Where health or adult social care data are involved, the incident may amount to a Serious Incident Requiring Investigation (SIRI) and require notification using NHS England procedures. This procedure applies to all health data WCTU is processing, and it is not limited to projects where there is an active Data Sharing Agreement (DSA) in place with NHS England. Further guidance on risk assessment and categorisation of a breach including risk scoring tools can be located here: https://www.dsptoolkit.nhs.uk/Help/29
For urgent security related incidents that require immediate advice and guidance a member of the investigation team should contact the Data Security Centre (formerly known as CareCERT) helpdesk immediately on 0300 303 5222 or contact enquiries@nhsdigital.nhs.uk. This activity and any resulting advice should be captured in the resulting Corrective and Preventative Actions (CAPA).

WCTU has a Data Security and Protection Toolkit (DSPT) which should be used to report incidents to NHS England. The reporting section of the toolkit can be accessed by the following link: https://www.dsptoolkit.nhs.uk. Access to the toolkit is password protected and reporting of incidences can be done by the following people:

- Head of Operations
- QA Managers
- Programming Team Manager

4.3.4.4 Notification to Sponsor & Insurance Services Manager

All breaches that originate from the UoW or a UoW Data Processor AND the DPO have determined this to be a breach that is reportable to the ICO or the data subject should be reported to the Sponsor representative and the Insurance Services Manager as soon as possible by sending details to Insuranceservices@warwick.ac.uk and Sponsorship@warwick.ac.uk. Otherwise, the Sponsor and Insurance Services Manager will receive a 6-weekly summary of all breaches via the WCTU report to the Sponsorship and Oversight Committee which is produced by the WCTU QA team.

4.3.5 Assessment of the incident by the WCTU investigation team

If the DPO assess the breach as one that should be reported to the ICO or the data subject, an investigation team should be set up with immediate effect withthe Head of Operations (or deputy) and a representative from the QA Team. Others may need to be included as necessary.. Where there are external/Co-Sponsors or External/Joint Data Controllers, they should also be notified and involved in the investigation. The team should try and establish as much information as possible and report the incident and in conjunction with the DPO's representative, the investigation should aim to establish the following:

- the root cause of the breach
- the scope of the breach
- the groups and numbers of individuals affected by the breach
- the categories of personal data affected by the breach
- whether the personal data affected were protected in any way (e.g. encrypted)

- the potential adverse consequences for the affected individuals
- any other consequences of the breach.

4.3.6 Corrective and Preventative Actions (CAPA)

Corrective and preventative actions required to contain and mitigate the breach will be identified, documented and undertaken. These may include:

- immediately recalling an email that has been sent to the wrong address or an incorrectly forwarded email chain
- contacting the recipient of an email that has been sent in error and asking them to delete the email from their inbox and deleted items and confirm they have done so
- immediately retrieving paper documents from any unintended recipients
- changing the password for the affected application, device, system or room
- immediately disabling any lost or stolen electronic devices
- notifying colleagues of any immediate steps that they should take
- remotely locating, disabling and/or deleting data stored on a mobile device
- restoring a database or system from a back-up
- disabling network or system access
- notifying staff and/or Processors to do or refrain from doing something

implementing the University’s business continuity and crisis management plans
Any suspected or actual breach, details of the investigation and any CAPA should be added to the WCTU non-compliance log using event type ‘data breach’ or ‘processor data breach’ as applicable. All actions need to be appropriate, proportionate and accountable and will be agreed under the guidance of the DPO or their nominated delegate. The notification date to the DPO should be included in the ‘Other bodies notified field. Recording the incident number from the autogenerated email is good practice.

4.3.7 Following the incident

Once all CAPAs are resolved, the incident will be considered closed, and the non-compliance log updated accordingly.

The non-compliance log will be regularly reviewed by the WCTU Governance Committee to ensure there are no systematic issues and that current preventative measures are appropriate.

Any lessons learnt from incidents will be shared where appropriate to improve security across WCTU and the wider University.

List of abbreviations

CAPA	Corrective and Preventative Actions
DPO	Data Protection Officer
DSA	Data Sharing Agreement
DSPT	Data Security and Protection Toolkit
GDPR	General Data Protection Regulation
ICO	Information Commissioners Office
PID	Personal Identifiable Data
QA	Quality Assurance
R&IS	Research & Impact Services
SIRI	Serious Incident Requiring Investigation
SOP	Standard Operating Procedure
UoW	University of Warwick
WCTU	Warwick Clinical Trials Unit