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

Version:	**3.0**	Effective Date:	23 June 2022
Issue Date:	09 June 2022	Review Date:	23 June 2024
Author:	Jill Wood, Quality Assurance (QA) Manager, WCTU		
WCTU Reviewers:	Ade Willis, WCTU Programming Team Manager		
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 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 Universities' central Breach Reporting Procedure. Where the University of Warwick is not a Data Controller for the personal data, the breach reporting procedures of the controller organisation should be consulted.

The procedures for managing data more generally are covered in SOP 15 (Information Handling) and all of its associated parts, which describes the procedure for managing data transfer, storage, and security of data.

The Universities 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/sim/policies/

If a personal data breach relates to a research study participant, it is likely to also satisfy the criteria of a protocol non-compliance, such as a violation or serious breach. If this is the case it must also be managed and reported in line with SOP 31 'Handling non-compliances, research misconduct and serious breaches of GCP and/or Study Protocol', although it is recommended that only one non-compliance report is created per incident.

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.
Personal Identifiable Data	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 in order to minimise impact.
Data Subject	The identified or identifiable living individual to whom personal identifiable data relates
Processor Data Breach	A Personal Data Breach (as defined above) that originates from a data processor.

	n.b. all the processors involved in a study should be detailed on the data flow map.
Data Controller	Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. 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	Act on behalf of, and only on the instruction of the relevant controller

3. Background

Data security 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

All members of staff that have access to or otherwise process personal data are responsible for reporting any personal data breach and for assisting with investigations where necessary.

University of Warwick Data Protection Officer (DPO)	• Overall responsibility for the management of the incidents and the decision as to whether a breach is reportable to the ICO
Head of Operations, QA Managers and Programming Team Manager	• Incident management involving WCTU • To convene as a response team for investigation of personal data breaches

For clinical trials, if the Personal Data Breach originates from an Investigator site, 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 follow their internal data breach procedures.

4.2 When?

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

Personal data incidents and breaches should be reported immediately to the QA team at WCTUQA@warwick.ac.uk who will support individuals to report the incident to the University's Legal and Compliance Team by following the guidance located here: https://warwick.ac.uk/services/legalandcomplianceservices/dataprotection/breaches.

Both Personal data breaches that originate from the University of Warwick or one of the University of Warwick's processors (Processor Data Breach) should be reported following the process in section 4.3. Processor data breaches only need to be reported where the University of Warwick is Sole or Co-controller.

It is very important to not delay and to contact the QA team and the Legal and Compliance team promptly. 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 will facilitate the process at WCTU.

4.3 How?

4.3.1 Types of incident

A personal data breach 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 person or 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 Assessment of the incident by the WCTU investigation team

Upon awareness of the breach or potential breach, an investigation team should be set up with immediate effect with those outlined in section 4.1. 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 immediately to the Legal and Compliance team as outlined in 4.2. The ongoing 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.

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

4.3.3 Reporting the breach

4.3.3.1 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 4.3.2. 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.

4.3.3.2 NHS Digital

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 Digital 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 Digital.

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 Digital. 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

Further guidance on how to report can be found in the link referenced in 4.3.2.

4.3.3.3 Sponsor & Insurance

All breaches that originate from the UoW should be reported to the Sponsor representative and the Insurance Services Manager as soon as possible by sending details to Insuranceservices@warwick.ac.uk.

4.3.4 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 potential or actual breach, details of the investigation and any CAPA should be added to the WCTU non-compliance log using event type 'Data Breach'. All actions need to be appropriate, proportionate and accountable and will be agreed under the guidance of the DPO or their nominated delegate.

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, for example, notification to a joint data controller or to the controller where the University of Warwick is the processor.

Other stakeholders may also need to be notified such as the Research Funders, data providers and the University Insurance Services Manager. If a criminal offence has been committed the police should be contacted. The Legal and Compliance Team will provide advice on who should be contacted and this should not be done until the actions are approved. The data subject should not be contacted until authorised to do so by the Legal and Compliance Team.

4.3.5 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
DPA	Data Protection Act
DPO	Data Protection Officer
DSA	Data Sharing Agreement
DSPT	Data Security and Protection Toolkit
GDPR	General Data Protection Regulation
ICO	Information Commissioners Office
QA	Quality Assurance
R&IS	Research & Impact Services
SIRI	Serious Incident Requiring Investigation
SOP	Standard Operating Procedure
WCTU	Warwick Clinical Trials Unit