Standard Operating Procedure (SOP)

MANAGEMENT AND USE OF USB DEVICES IN RESEARCH DELIVERY

SETTING Trust wide

AUDIENCE Research staff responsible for delivering both commercial and non-commercial research at UHBW.

ISSUE The use of USB devices presents an IT security risk to the Trust, and their use is tightly controlled. However, some research studies require the use of secure USB devices supplied by external sponsors. In these cases, the use of USB devices must adhere to all relevant laws, regulations, and Trust policies, as well as Good Clinical Practice (GCP) requirements.

QUERIES Contact R&D department: research@uhbw.nhs.uk

Document History

SOP number	SOP 030	**SOP Version**	1.0
Effective Date	24/APR/2026	**Review Date**	24/APR/2028

Review date	Version number	Version date	Effective date	Author/ Reviewer	Authorised by
N/A - original	1.0	15/JAN/2026	24/APR/2026	Rosina Jarvis Nicola Manning	Diana Benton (on behalf of TRG)

Version Number	Reason for change
Original V1.0	N/A Original

1. Introduction

USB access is considered a security risk for the trust as it provides an access route for malware and can lead to data leakage. As per NHS digital guidance “access to removable media should be prevented as far as practicable, as it can be used to transport untrusted content.” (NHS England, 2022).

Research studies are run across the trust in conjunction with study sponsors. Sponsors are individuals, organisations or partnerships that have overall responsibility for healthcare research studies (NHS Health Research Authority, 2023). When working with these outside parties it is sometimes necessary to use USB devices to collect, produce and/or share data. The USB devices are provided by the sponsor and maintained by the sponsor throughout the study.

As part of both commercial and non-commercial research studies data is collected on patients who have consented to take part in research. This data is shared with the sponsor of the study securely through online databases that have been set up for the specific purpose of the study. These databases are secured by passwords and where possible two-factor identification is used to ensure security of the data. In certain circumstances a USB is required to download data from an externally provided device which is unable to connect to NHS systems (for security reasons) and that data then requires upload onto the secure sponsor database. A USB may also be provided by sponsor to share required study information (e.g. training slides of study documents).

Any data shared with the sponsor is laid out in the study protocol, patient information sheet and consent form and must adhere to Good Clinical Practice guidelines (NHS Health Research Authority, 2020). Where possible personal identifiers are removed from any data and each patient is allocated a study Identification number/code.

2. Purpose

The purpose of this SOP is to provide research delivery staff with guidance on the authorised procedures for using USB devices on Trust systems during research activities, to minimise security risks and ensure safe data handling

3. Scope

In Scope: USB devices provided by study sponsor for essential research activities.
Out scope: Personal USB devices

4. Responsibilities

All research staff using USB devices for research purposes are responsible for ensuring that the SOP is followed and that the use of USB device is necessary and complies with the requirements in this SOP.

5. Abbreviations and Definitions

Abbreviations	
GCP	Good Clinical Practice
MEMO	Medical Equipment Management Organisation
R&D	Research and Development
USB	Universal Serial Bus

6. Procedure

6.1 Requesting and Approving USB Devices

- When notified that a USB device is required for a study, confirmation that the sponsor holds valid insurance and can supply a secure, compliant USB device should be sought.
- Only USB devices issued by the sponsor and deemed trusted may be used for research activities.

6.2. Receiving the USB Device

Upon receipt of the device:

- Ensure the USB device is checked and/or registered with IT and MEMO in line with Trust requirements.
- Maintain a departmental register of all high-value devices received, for inclusion in the emergency evacuation and fire plan.
- Ensure the USB device remains on Trust premises wherever reasonably practicable.

6.3. Using the USB Device

- Limit access to the USB device to authorised research delivery staff only, and remove access when it is no longer required.
- Use the minimum necessary personal identifiers when storing or transferring data on the USB device.
- Only upload data from the USB device to secure, sponsor-managed databases in line with requirements of the approved Protocol.

6.4. Returning the USB Device

- Follow the study protocol guidance for returning USB devices to the sponsor.
- Update the departmental USB device register to record the date the device was returned.

7. Dissemination and training in the SOP

This SOP should be disseminated to applicable research staff (including R&D) and should be available on the R&D website.

Definitions	
Standard operating procedures	Detailed, written instructions to achieve uniformity of the performance of a specific function.
USB	A standardised technology for attaching peripheral devices to a computer.

Plan Elements	Plan Details
The Dissemination Lead is:	Research Operations Manager
Is this document: A – replacing the same titled, expired SOP, B – replacing an alternative SOP, C – a new SOP:	C – a new SOP
If answer above is B: Alternative documentation this SOP will replace (if applicable):	
This document is to be disseminated to:	All applicable research staff (including R&D)
Method of dissemination:	For major updates to the SOP dissemination will be: 1. To Chief Investigators of UHBW Sponsored CTIMPs 2. Research Unit leads across UHBW 3. Head of Research Governance at UoB (where SOP is applicable) All updates (major and minor to the SOP) will be: 1. Updated on the trust Document Management System 2. Updated on the R&D website 3. Cascaded in R&D communications
Is Training required:	All staff whose activities are subject to this SOP should ensure that they read and understand the content of the SOP. The personal training log of the individual (and the Investigator Site File/Trial Master File if required) should be completed to document that the content of this SOP has been read and understood as described in *SOP_007 Research Training UHBW*

REFERENCES	NHS Health Research Authority (2020) Good Clinical Practice. Available at: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/good-clinical-practice/ NHS England (2022) NHS Digital, Guidance on protecting connected medical devices, step 3 Apply mitigations to reduce the likelihood of compromise. Available at: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-connected-medical-devices/step-3.-apply-mitigations-to-reduce-the-likelihood-of-compromise

	NHS Health Research Authority (2023) UK policy framework for health and social care research. Available at: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/uk-policy-framework-health-social-care-research/uk-policy-framework-health-and-social-care-research/#sponsors
RELATED DOCUMENTS AND PAGES	Acceptable Use of IT Policy https://uhbw.mystaffapp.org/6442/document_view.pdf Validation and backup of computer systems used in research SOP https://uhbw.mystaffapp.org/15214/document_view.pdf Information Security Policy https://uhbw.mystaffapp.org/13446/document_view.pdf Information Governance Policy https://uhbw.mystaffapp.org/13810/document_view.pdf
AUTHORISING BODY	Trust Research Group
SAFETY	
QUERIES AND CONTACT	Contact the Research & Development department via research@uhbw.nhs.uk
AUDIT REQUIREMENTS	R&D departmental Quality Management System audits are undertaken annually.