York and Scarborough Teaching Hospitals NHS Foundation Trust R&D Unit
SOP
R&D/S66

External Monitoring Visits

IT IS THE RESPONSIBILITY OF ALL USERS OF THIS SOP TO ENSURE THAT THE CORRECT VERSION IS BEING USED

All staff should regularly check the R&D Unit's website and/or Q-Pulse for information relating to the implementation of new or revised versions. Staff must ensure that they are adequately trained in the new procedure and must make sure that all copies of superseded versions are promptly withdrawn from use unless notified otherwise by the SOP Controller.

The definitive versions of all R&D Unit SOPs appear online. If you are reading this in printed form check that the version number and date below is the most recent one as shown on the R&D Unit website: www.research.yorkhospitals.nhs.uk/sops-and-guidance-/ and/or Q-Pulse

SOP Reference:	R&D/S66
Version Number:	1.0
Author:	Monica Haritakis
Implementation date of current version:	16th August 2023

Approved by:	Name/Position:	Lydia Harris, Head of R&D
	Date:	19th July 2023
	Name/Position:	Sarah Sheath, SOP Controller
	Date:	19th July 2023

This SOP will normally be reviewed at least every 3 years unless changes to the legislation require otherwise

Version History Log

This area should detail the version history for this document. It should detail the key elements of the changes to the versions.

Version	Date Implemented	Reviewers	Details of significant changes
1.0	16th August 2023		

Contents

1 Introduction, Background and Purpose

Monitoring is the act of overseeing the progress of a study and of ensuring that it is conducted, recorded and reported in accordance with the protocol and any amendments, written procedures, Good Clinical Practice (GCP), and the applicable regulatory requirements.

Monitoring is one of the key mechanisms whereby the Sponsor can be assured that:

- the safety, right and well-being of trial subjects are protected

- investigators are appropriately selected, trained and supported to complete the proposed clinical trial

- processes are consistently followed and activities are consistently documented to ensure high-quality trial conduct and protocol compliance

- the reported trial data are accurate, complete, and verifiable against the source documents

- the conduct of the trial is in compliance with the currently approved protocol/ amendment(s), with GCP and with the applicable regulatory requirement(s).

The purpose of this SOP is to describe the procedures for preparing for external monitoring of research studies hosted by the Trust.

2 Who Should Use This SOP

This SOP should be used by staff arranging and facilitating on site or remote monitoring by the study Sponsor.

3 When this SOP Should be Used

The SOP should be used by investigators and relevant research staff in preparation of external monitoring visits of hosted research studies by a monitor from the study sponsor or Clinical Research Organization.

4 Procedure(s)

4.1 On-site Monitoring

Upon notification of the monitor's visit, inform the Principal Investigator, key study personnel and staff from applicable support services about the visit. e.g., pharmacy and labs.

4.1.1 <u>Before the Monitoring Visit</u>

- Arrange a suitable date for the visit and send an invite to all relevant staff.

- Book a room for the monitor to review the study documents during the visit.
- Ensure that the PI has time set aside to meet with the monitor and/or to follow-up from the monitoring visit.
- Identify what documents will be reviewed during the visit and ensure that these will be available.

4.1.2 During the Monitoring Visit

- Verify the identity of the monitor upon arrival.
- Escort the monitor to the room.
- Inform the monitor about access to restrooms, water, any safety and emergency instructions and study staff availability or contact information, as appropriate.
- Confirm PI interview time (if relevant)
- Provide over the shoulder access to CPD
- Provide assistance with any queries.
- If required guide the monitor to relevant support services.

4.1.3 After the Monitoring Visit

- Return all study documents to the secured locations.
- Ensure that a follow up letter or monitoring report is received from the monitor.
- Send a copy of the report to the Research QA team for review.
- Review the findings in the monitoring report with the PI and key study personnel and have the PI sign the letter. Develop any necessary Corrective and Preventative Action (CAPA) plans.
- Prepare complete responses to any findings in the monitoring report and send the requested corrections or responses to the monitor.
- Place a copy of the monitoring and site response reports in the ISF.

4.2 Remote Monitoring

There may be the requirement to complete remote monitoring for some studies. This may involve sending pseudonymised copies of source data documents by encrypted email or hosting a remote visit by Microsoft Teams or a combination of these. Alternatively, Sponsors may provide a remote monitoring checklist that can be completed and returned to them by email.

4.2.1 Monitoring via Microsoft Teams

Please note: With remote monitoring via Microsoft Teams, source documents may be shown to the camera/or screen share functionality used, but recording MUST NOT take place. Taking a screenshot is also NOT allowed.

Where a remote visit is required, this must be completed using Microsoft Teams. Prior to attending the remote visit the external research Monitors/ Associates/ Inspectors will be required to complete the Remote Source Data Verification (SDV) Agreement (R&D/T50). This must be returned to Research Governance for agreement by the Research QA Manager. Once agreement is received that the visit

can go ahead a date can be arranged and an invite should be sent to the external monitor by the relevant member of the research team.

On the date of the remote visit the research team must verify the identity of the monitor and ensure that no unauthorised individuals are on the call. The monitor must be advised that video recording and taking screenshots is not allowed.

If there are any disclosures of data not covered by the Remote SDV Agreement these must be reported to Research Governance aa soon as possible and an DATIX must be completed as described in the Research Related Adverse Incident Reporting SOP (R&D/S112).

4.2.2 Use of encrypted email

Please refer to section 7. Appendix B for encryption instructions that are used within the Trust.

Encrypted emails can be used for sharing pseudonymised copies of source data documents (redacted and replaced by a study identifier). Encrypted emails are sent using TrendMicro encryption - NHS Encryption. Before sending patient or sensitive data via the encryption service, 'encrypted channel' must be set up which allows safely verify the correct recipient. The service will then encrypt the message and deliver it to the intended recipient. Full details can be found in appendix.

Please Note: The R&D Unit requires a second site staff member to check the redaction before disclosure to a study monitor/auditor and Sponsors. In case of using redacted documents, York Trust sites need to keep the redacted documents in the ISF/or e-ISF including the date when they were used for remote SDV.

5 Related SOPs and Documents

R&D/T50 Remote Source Data Verification (SDV) Agreement

R&D/F17 Monitoring Visit Log

R&D/S112 Research Related Adverse Incident Reporting

6 Appendix B – Encryption Services Instructions

If users need to exchange information securely outside of the above secure email boundary, they can do so by using the NHSmail encryption feature.

Encryption should primarily be used to exchange sensitive data as part of an agreed clinical workflow, and users should follow any local Information Governance policies that in place locally for sending sensitive data.

Before sending patient or sensitive data via the encryption service, it is good practice to set up the 'encrypted channel' which helps safely verify the correct recipient.

1. First, send the recipient the 'Encryption Guidance for recipients' document which you can find in the NHSmail Training and Guidance pages at: https://support.nhs.net/knowledge-base/accessing-encrypted-emails-guide-for-non-nhsmail-users/

2. Next, follow the steps below to send an initial encrypted email but do not include patient or sensitive information. Once the recipient of the information has registered for the encryption service and confirmed to the sender this has been done, patient and sensitive data can be sent within an email or as an attachment subject to local information governance policies.

3. To send an encrypted email, ensure you are using an NHSmail account and create a new email message in the normal way.

4. Ensure the recipient's email address is correct.

5. In the 'Subject' field of the email, enter the word [secure] before the subject of the message. The word secure must be surrounded by the square brackets for the message to be encrypted. If square brackets aren't used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment.

6. Compose the message.

7. Add any required attachments (once the initial registration process has taken place).

8. Click on Send to send the message. An unencrypted copy will be saved in your Sent Items folder.

The service will then encrypt the message and deliver it to the intended recipient. The sent item will be stored unencrypted in your Sent Items folder, and any replies received will be decrypted and displayed as normal in NHSmail. N.B. [secure] is not case sensitive and [SECURE] or [Secure] for example could also be used.
For help or further advice please visit Trend Micro support site at:
http://www.privatepost.com/support/faqs.aspx

or call the national NHSmail helpdesk on 0333 200 1133 or email helpdesk@nhs.net
Recipients of NHSmail encrypted emails who require help with registration should refer to the help provided on the registration website.