

Electronic Signature

SOP Reference: RGIT_SOP_043	
Version Number: 3.0	
Effective Date: 22 Jul 2022	Review by: 19 Oct 2023
Author: Rosemary Ichaba, Quality Assurance Facilitator	
Approved by: Ruth Nicholson, Head of Research Governance and Integrity	Date:

Version	Date	Reason for Change
Version 1.0	21 April 2020	1 st Edition
Version 2.0	19 Oct 2020	Scheduled Review Administrative changes to SOP. JRCO name change to RGIT.
Version 3.0	22 Jul 2022	Further clarification made to the process of electronic signatures

Table of Contents

1. PURPOSE	3
2. INTRODUCTION	3
2.1. European Medicines Agency (EMA) Introduction of digital signatures 3	
2.2. Medicines & Healthcare products Regulatory Agency (MHRA)	3
3. RESPONSIBILITIES	4
4. PROCEDURE	4
4.1. Creating the digital Signature	4
4.2. Applying the E-signature to a Document	6
5. REFERENCES	7
6. APPENDICES	7

1. PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to describe the procedure of using Electronic signatures (E-signature) in documents.

2. INTRODUCTION

There are several documents which are created for the set-up and management of research studies that will require a signature. The process of gaining a signature certifies that the document adds value and can be used to approve, review and validate certain events or actions that may occur throughout the duration of the research. The existing process of signing documents as 'wet ink' will be a process that will still be utilised but for a certain number of documents. The following documents listed below can be considered as mandatory wet-ink signed documents, but may also be considered by a case by case basis:

- Protocols and Amendments
- Consent forms
- Completed Case report forms
- CRF correction signature sheet/ signature logs

Electronic signatures can be accepted for agreements and contracts but there may be some cases where a wet ink signature may also be required if the sponsor deems it necessary. However, if in doubt, double check with the college/trust contracts team on a case by case basis. As referenced in section 2.2 MHRA of this SOP any: *use of an inserted image in place of a signature to indicate the document has been signed electronically will not be an adequate form of the signature process therefore these should not be used for MHRA study/documents.* However, based on the risks level of studies/documentations outside MHRA e.g. non-CTIMP studies standard e-signatures (including insertion of an image) may still be adequate for use provided it can be verified and an adequate process is in place to ensure changes to the documents will then invalidate the signature.

The process of e-signatures can be completed using either a validated system e.g. DocuSign, verified e-signature (see notes above), Acrobat or Adobe reader which is described in section 4. The PDF e-signature process is able to capture the date, time and signee of the document; producing an audit trail of signatures.

2.1. European Medicines Agency (EMA) Introduction of digital signatures

The EMA decided to introduce the use of digital signatures in September 2013 for outgoing documents that require a legally binding signature. The EMA have put in place a strategy to increase electronic documents between the pharmaceutical industry and the Regulatory bodies. The EMA have creating a service to test PDF electronic documents and the criteria for exchanging signed electronic documents which can be found on their website: [e submission EMA Europa](#) (cited 18 June 2020)

2.2. Medicines & Healthcare products Regulatory Agency (MHRA)

The MHRA have also produced guidelines to assist with the use of electronic signatures in March 2018. The appropriate validation of the signature will need to be

demonstrated to ensure control over the signed records can be maintained; this means the metadata associated with the electronic signature must be maintained within the associated signed document. The MHRA have defined metadata to be “Metadata is data that describe the attributes of other data, and provide context and meaning. Typically, these are data that describe the structure, data elements, interrelationships and other characteristics of data. It also permits data to be attributable to an individual”. In this context, the metadata needed to validate a signature can include the users name, date, time and sometimes location.

The use of an inserted image in place of a signature to indicate the document has been signed electronically will not be an adequate form of the signature process. Therefore, it is essential that the metadata is retained within the document for the electronic signature to be valid.

The MHRA have included within the 2004 Regulations that the acceptance of electronic signatures for consent can also be valid but will depend on the type of electronic signature that will be required. Further information can be found in the Joint Statement on Seeking consent by Electronic Methods guidance by the HRA and MHRA – Version 1.2: September 2018.

3. RESPONSIBILITIES

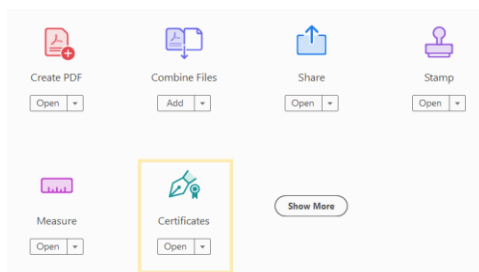
This SOP is to be followed by any staff involved in the management of RGIT sponsored CTIMPs and non-CTIMPS studies. Alongside any staff working within the RGIT unit.

4. PROCEDURE

4.1. Creating the digital Signature

Please see the screenshots below which demonstrate the following instructions:

1. Open the created PDF file and navigate to the “Tools” tab on the top left side.
2. Click on the “Certificates” icon



3. Click on “Digitally Sign” option






4. Highlight the area where you would like to place the signature





- *How to configure your new digital ID?*
 - i. Click “Configure digital ID”
 - ii. Select the “Create a new digital ID” option

Select the type of Digital ID:

-  **Use a Signature Creation Device**
Configure a smart card or token connected to your computer
-  **Use a Digital ID from a file**
Import an existing Digital ID that you have obtained as a file
-  **Create a new Digital ID**
Create your self-signed Digital ID


- iii. Select the “Save to Windows Certificate store” as the destination

-  **Save to File**
Save the Digital ID to a file in your computer
-  **Save to Windows Certificate Store**
Save the Digital ID to Windows Certificate Store to be shared with other applications

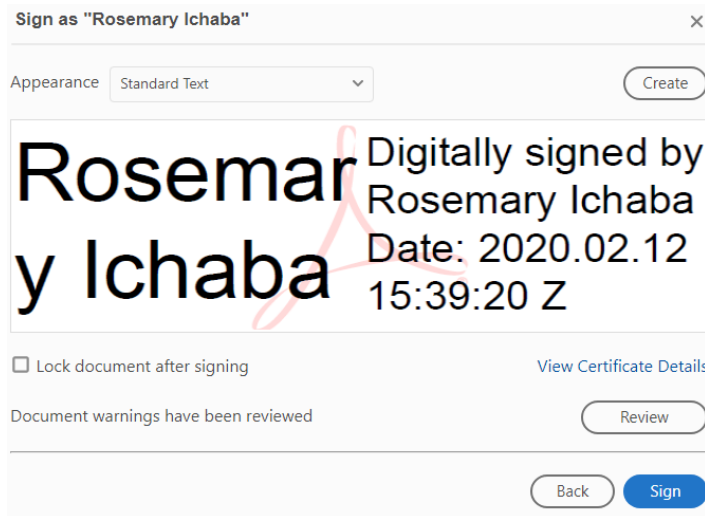
- iv. Enter the required information and ensure the Country/Region has been correctly selected
- v. Click save

5. Now the Digital ID has been created you can choose an ID for signature

Choose the Digital ID that you want to use for signing:

-  **Rosemary Ichaba (Windows Digital ID)**
Issued by: Rosemary Ichaba, Expires: 2025.02.12

6. Once an ID has been selected click “Continue”
7. A preview of the signature will appear, click “Sign”



8. The signed document can then be saved in the desired location with the metadata displayed.

4.2. Applying the E-signature to a Document

4.2.2. Applying a signature to a Word document

1. Open the desired word document, click file and then “save as”.
2. Change the file format from word document to “PDF”.
3. Ensure the name of the document is correct and click save.
4. Navigate to the location of the saved PDF and open the document.
5. Click “Tools” on the top left tab and then click “Certificates”.
6. Click “Digitally Sign” and highlight the area where you would like the signature placed.
7. As you have created a digital ID, following the steps in [Section 4.1](#), “Creating the digital Signature”, you should be able to choose your digital ID signature and click continue.
8. Confirm that the signature name and date/time stamp (metadata) is correct and click Sign.
9. You may be required to rename the signed document to ensure the document with the signature has been saved.
10. Your signature should now be applied in the document and saved.

4.2.3. Applying a signature to a Scanned document

1. Locate the scanned document and ensure that the document has been saved as a PDF Formatted document.
2. If the document is not saved as a PDF, right click the document and click “open with”. Within the list of options, navigate to Adobe and proceed to open the document using the Adobe Application.
3. Save a copy of the document as a PDF.

4. Once the document has been saved correctly, you can now follow steps 5-10 within section 4.2.2. *Applying a signature to a word document.*

5. REFERENCES

[European Medicines Agency \(EMA\) Introduction of digital signatures](#)

[Medicines & Healthcare products Regulatory Agency \(MHRA\) 'GXP' Data Integrity Guidance and Definitions – Revision 1: March 2018 \(cited date: 23 Sep 2020\)](#)

[Joint Statement on Seeking Consent by Electronic Methods v1.2 September 2018 \(cited date; 23 Sep 2020\)](#)

[MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015 \(cited date: 21 Jul 2022\)](#)

6. APPENDICES