

Joint Research Management Office Standard Operating Procedure for:

Guidance documents for e-signatures

Number:	N/A – Guidance Document	Version Number:	1.0
Effective Date:	2nd January 2023	Review Date:	2nd January 2024

Authorship & Review:		Signature & Date:
Author:	Rebecca Carroll Quality Assurance Manager	
Reviewer:	Marie-Claire Good, Senior GCP and Governance Manager	

Authorisation:		Signature & Date:
Name/Position	Mays Jawad Research Governance Operations Manager	

Background:

Due to the implications of remote working, the process of obtaining wet signatures has become impractical and alternative methods of ensuring document validation was sought.

Purpose:

The purpose of this guidance document is to describe the procedure of using electronic signatures (e-signature) in pertinent documentation where wet signatures were normally obtained.

Scope:

This guidance is mandated for all sponsored MHRA Regulated study documents. A CTU/Study Group can use an established, equal e-signature process to this guidance once agreed by the GCP and Governance Manager, e.g., DocuSign or Adobe Signature.

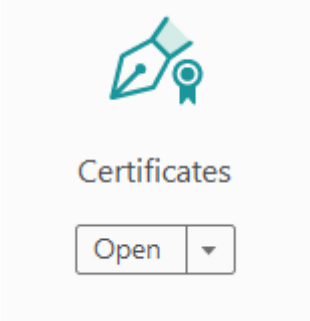
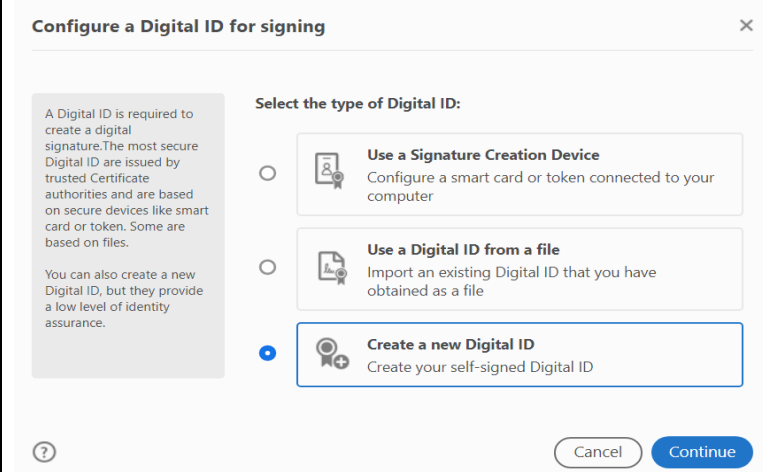
For sponsored Interventional and Research study documents, this guidance is mandatory for all sponsor to CI documents and best practice for all other documents.

This document also acts as a guidance documents for all research within Barts Health and Queen Mary.

Please note, the JRMO does not advocate the use of fill and sign nor cut and paste as acceptable forms of digital signatures.

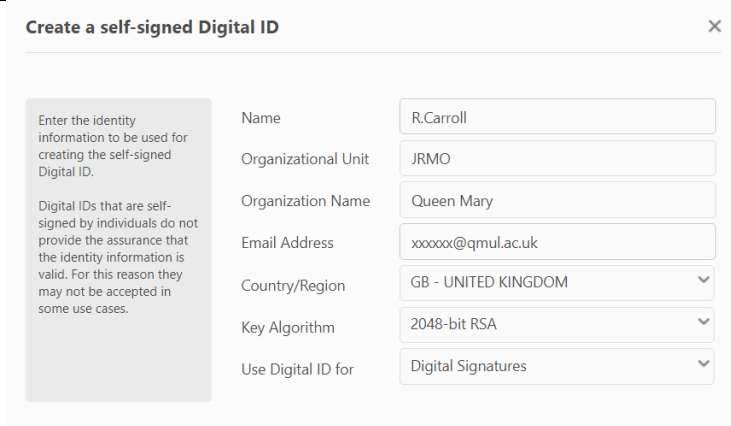
Abbreviations:

Barts Health	Barts Health NHS Trust
Queen Mary	Queen Mary University of London

	Activity
1.	<p>Following risk based review of guidance from both the MHRA and HRA, documentation falling under the scope of this guidance document required advances electronic signatures (Signatures that are uniquely linked to the signatory, are capable of identifying the signatory, allow the signatory to retain control, and are linked to data within the signature that can detect any changes made).</p> <p>The JRMO has therefore accepted use of an e-signature certificate using Adobe Acrobat Reader.</p> <p>The e-signature process will provide an audit trail of the signatures which will include signee, date and time.</p> <p>This platform allows more than one signature per document with the ability to check the signature validation status and also the signature panel for the whole document.</p>
2.	<p>Creating an e-signature certificate</p> <ul style="list-style-type: none"> Open the pdf using Adobe Acrobat Reader Click on More Tools in the left-hand corner and select certificates Select digitally sign. Draw the area/text box where you would like the signature to appear. Once done there will be an option to sign with a digital ID. 
3.	<p>Create a new Digital ID</p> <ul style="list-style-type: none"> Select configure New Digital ID. Select create a new digital ID and continue. Select save to file. You will be prompted to create a self-signed digital ID. Your digital ID must be your full name. Complete the details appropriately.  <ul style="list-style-type: none"> Create a password for the Digital ID and save and select continue. You will see a preview of the signature. There is the option to lock the document following signature if this is required. Do not select lock if multiple signatures are required on one document.

- Enter the password and select sign.

There will be a prompt to save the document. Once saved, the signature certificate will appear in the text box previously created.



Create a self-signed Digital ID

Enter the identity information to be used for creating the self-signed Digital ID.

Digital IDs that are self-signed by individuals do not provide the assurance that the identity information is valid. For this reason they may not be accepted in some use cases.

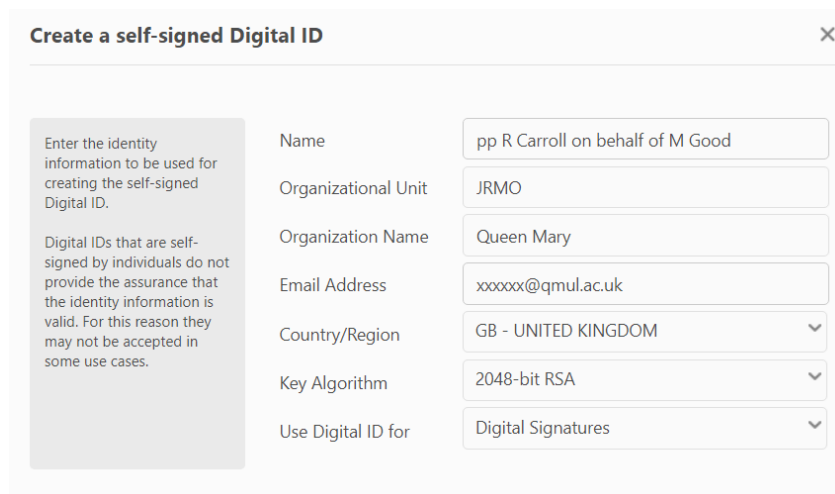
Name	R.Carroll
Organizational Unit	JRMO
Organization Name	Queen Mary
Email Address	xxxxxx@qmul.ac.uk
Country/Region	GB - UNITED KINGDOM
Key Algorithm	2048-bit RSA
Use Digital ID for	Digital Signatures

R Carroll Digitally signed by R Carroll
Date: 2022.08.19 13:48:23 +01'00'

4. Further use of e-signatures

The e-signature is saved on your local PC account and can be used for further e-signatures. The time and date will update accordingly.

Where there is a need to sign on another staff members behalf, an e-signature certificate can be created as described in section 2 and 3 however it must clearly state when prompted to complete the Digital ID, both names are clearly noted (See images below). There must also be evidence that this form of signature authorisation has been agreed by both parties. It is not acceptable to sign digitally on someone else's behalf where the individual's password for the Digital ID has been shared.



Create a self-signed Digital ID

Enter the identity information to be used for creating the self-signed Digital ID.

Digital IDs that are self-signed by individuals do not provide the assurance that the identity information is valid. For this reason they may not be accepted in some use cases.

Name	pp R Carroll on behalf of M Good
Organizational Unit	JRMO
Organization Name	Queen Mary
Email Address	xxxxxx@qmul.ac.uk
Country/Region	GB - UNITED KINGDOM
Key Algorithm	2048-bit RSA
Use Digital ID for	Digital Signatures

pp R Carroll on behalf of M Good Digitally signed by pp R Carroll on behalf of M Good
Date: 2022.08.19 13:45:03 +01'00'

References:

1. MHRA 'GXP' Data Integrity Guidance and Definitions

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf

2. HRA Joint statement on seeking consent by electronic methods

<https://s3.eu-west-2.amazonaws.com/www.hra.nhs.uk/media/documents/hra-mhra-econsent-statement-sept-18.pdf>