Division of Population Health Certified Data Deletion Procedure

This version (v2.3) Approved at IG Committee Meeting 2024-02-26

This process should be read in conjunction with the document "Technical description of what happens when files are deleted" that describes what happens when a file is deleted.

Division of Population Health process for requesting certified data deletion:

For data held in a project folder on the X drive (where all contents of the folder are to be deleted)

Project team:	The IAO or a Deputy will contact Division of Population Health DS to say that there are data on the X drive that need deleting for which a deletion certificate is required. Give Division of Population Health DS the project details (name of project and name of X drive folder), the name of the person on the project team who will be dealing with the process. State explicitly that *all* contents of the folder need to be deleted.
Division of Population Health DS:	Remove all access to the control folder except for the designated person on the project team.
Project team:	Delete all contents of the original folder.[1]
Division of Population Health DS:	Remove all project team access to the original control folder and request deletion from Storage & Server.
Storage & Server Team	Delete folder and notify Division of Population Health DS.
Division of Population Health DS:	Update records and notify Project Team that folder has been deleted.
IG lead / IG manager:	Confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by the data provider, e.g. NHS England). Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.

[1] If Storage & Server find files in the folder, they will bounce the request back. This is a safeguard to prevent them from accidentally deleting the wrong folder, because once it's gone, it's gone.

IG lead / IG manager:	Complete and sign the certificate of data destruction (see example NHS Digital Certificate of Data Destruction if applicable) and send to project team; include the details of the data to be destroyed, as outlined in the data sharing agreement (DSA).
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send the certificate to the data provider if required. Provide the IG lead / IG manager with a copy.
IG lead / IG manager:	File the completed certificate of data destruction within the destruction certificates folder on the IG - private Google Drive.

In summary, the project team deletes the contents, Division of Population Health DS removes access, and the Storage & Server team delete the actual folder and its associated Active Directory groups from the server, which prevents recovery without recourse to the emergency backups, and so can be considered securely deleted.

For data held in a project folder on the X drive (where *not* all of the contents of the folder are to be deleted)

Project team:	The IAO or a Deputy will contact Division of Population Health DS to say that there are data on the X drive that need deleting for which a deletion certificate is required. Give Division of Population Health DS the project details (name of project and name of X drive folder), the name of the person on the project team who will be dealing with the process. State explicitly that *not* all contents of the folder need to be deleted. Be aware that in order to be secure, the whole folder must be deleted, not just selected data from within it. Any files that are not to be deleted must first be copied to an alternative location, before the original folder is securely deleted.
Division of Population Health DS	Create a new control folder within the project shared area. Give access to the new folder to all users who have access to the old folder. Remove all access to the old folder except for the designated person on the project team.
Project team:	Copy (not move) all files that are to be retained into the new control folder. Delete all contents of the original folder.[2]

[2] If Storage & Server find files in the folder, they will bounce the request back. This is a safeguard to prevent them from accidentally deleting the wrong folder, because once it's gone, it's gone.

Division of Population Health DS:	Remove all project team access to the original control folder and request deletion from Storage & Server.
Storage & Server Team	Delete folder and notify Division of Population Health DS.
Division of Population Health DS:	Update records and notify Project Team that folder has been deleted.
IG lead / IG manager:	Confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by the data provider, e.g. NHS England). Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.
IG lead / IG manager:	Complete and sign the certificate of data destruction (see example NHS Digital Certificate of Data Destruction if applicable) and send to project team; include the details of the data to be destroyed, as outlined in the data sharing agreement (DSA).
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send the certificate to the data provider if required. Provide the IG lead / IG manager with a copy.
IG lead / IG manager:	File the completed certificate of data destruction within the destruction certificates folder on the IG - private Google Drive.

In summary, all files to be retained are copied into a new folder, the project team deletes the contents of the original folder, Division of Population Health DS removes access, and the Storage & Server team delete the actual folder and its associated Active Directory groups from the server, which prevents recovery without recourse to the emergency backups, and so can be considered securely deleted.

For data held in a VM filestore where Division of Population Health-DS have admin rights to the VM

Project team:	Copy files that are to be kept into a new location (typically, an X drive project folder) that has appropriate access permissions (this should not include the original data, and if it includes derived data this must have been confirmed as such by the data provider according to their process). **Anything left in the VM filestore will be deleted.**
Project team:	Shut down VM. Start menu >  > Shut down

Project team:	Contact Division of Population Health DS to say that there are data in a VM filestore that need deleting for which a deletion certificate is required. Give Division of Population Health DS the project details (name of project and name of the VM).
Division of Population Health DS:	Contact IT Services to delete the VM and VM filestore.[3]
Division of Population Health DS:	Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.
IG lead / IG manager:	Confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by the data provider).
IG lead / IG manager:	Complete and sign the certificate of destruction (see example NHS Digital Certificate of Data Destruction if applicable) and send to the project team; include the details of the data to be destroyed, as outlined in the DSA.
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send the certificate to the data provider if required. Provide the IG lead / IG manager with a copy.
IG lead / IG manager:	File the completed certificate of data destruction within the destruction certificates folder on the IG - private Google Drive.

For data held in a VM filestore where Division of Population Health-DS do not have admin rights to the VM

Project team:	Copy files that are to be kept into a new location (typically, an X drive project folder) that has appropriate access permissions (this should not include the original data, and if it includes derived data this must have been confirmed as such by the data processor according to their process). **Anything left in the VM filestore will be deleted.**
Project team:	Shut down VM. Start menu >  > Shut down
Project team:	Contact IT Services to delete the VM and VM filestore.[3]
Project team:	Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.

[3]IT Services routinely put VM deletion requests 'on hold' for two weeks unless they are specifically asked to circumvent their normal procedure

IG lead / IG manager:	Confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by the data provider).
IG lead / IG manager:	Complete and sign the certificate of data destruction (see example NHS Digital Certificate of Data Destruction if applicable) and send to the project team; include the details of the data to be destroyed, as outlined in the DSA.
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send the certificate to the data provider if required. Provide the IG lead / IG manager with a copy.
IG lead / IG manager:	File the completed certificate of data destruction within the destruction certificates folder on the IG - private Google Drive.

For data held in the Secure Data Service

Project team:	Contact the Secure Data Service (SDS) team regarding data destruction. Be aware that the preference of the SDS team is to delete the whole drive or bucket, not just selected data from within it. Any files that are not to be deleted must first be copied to a new drive or bucket, before the original drive or bucket is deleted entirely by the SDS team.
SDS team:	Ensure data destruction is carried out and documented in accordance with the documented process maintained by the SDS team.
Project team & IG lead / IG manager:	If additional certification is required: obtain Topdesk ticket from SDS team confirming deletion. Complete, sign, send and file the certificate of data destruction as described in other sections above.

Version	Effective Date	Summary of changes
1.0	08-May-2020	n/a first version
2.0	24-Jan-2022	Updated to include the DSH. Process to delete X drive data updated to protect the data from recovery.
2.1	30-Mar-2023	Updated to be more generic and cover data destruction for providers other than NHS Digital (now NHS England (merger 1st Feb 2023), but a new template hasn't been issued yet). Also Data Safe Haven is now the Secure Data Service. Other minor typographical changes made.
2.2	22-Jan-2024	Footnotes and clarification added to explain the process of data deletion prior to folder destruction. Footnote added to explain IT Service policy of waiting two weeks before deleting VMs. ScHARR replaced with Division of Population Health.

		Added details of where the destruction certificates are filed. Division of Population Health DS do not get involved where they do not have admin rights to the VM, therefore they've been removed from the process.
2.3	26-Feb-2024	Clarification of destruction process for SDS; further clarification regarding deleting entire folder added to X drive section.