

**CERTIFICATE OF DISPOSITION (COD)  
FOR DATA ACQUIRED FROM THE CENTERS FOR MEDICARE AND MEDICAID SERVICES (CMS)**

**DUA Requester**

*Must match the individual specified in the DUA.*

**Requesting Organization**

*Must match the organization specified in the DUA.*

**Study Title**

*Must match the study title specified in the DUA.*

**DUA #**

**GENERAL INSTRUCTIONS**

The DUA Requester or Data Custodian must complete this certificate if they wish to:

- Close the entire DUA and all associated files; or
- Close certain files on the DUA but leave the DUA and the remainder of its files open; or
- Document destruction of physical media

By completing this certificate, the DUA Requester or Data Custodian certifies that the Requesting Organization has destroyed/discontinued use of CMS data specified on this form at all locations. This includes any original files, copies, derivatives or subsets, and any back-ups. The Requesting Organization may not retain any copies, derivatives or manipulated files unless approved by CMS for use on another open CMS DUA. The Requesting Organization may retain data that is de-identified under the HIPAA Privacy Rule as described at 45 CFR 164.514(b) and adheres to CMS policy for cell size suppression.

Please ensure the Requesting Organization has completed one of the following approved methods to dispose of CMS data:

- Clearing - sanitize data or media using organizationally approved and validated technologies, methods, or tools. Clearing shall render data unrecoverable in the service or medium in which it is stored; either by cryptographic means (e.g., sanitizing the encryption key for a cloud storage service) or the equivalent, such as overwriting, resetting, or other measures to prevent data recovery.
- Purging - degauss with an organizationally approved degausser rated at a minimum for the media. Other methods of purging include overwrite, block erase, and cryptographic means using techniques that apply service-specific methods to bypass the abstraction inherent in typical read and write capabilities of services or devices (e.g., cloud storage or physical devices).
- Destroy - shred, disintegrate, melt, pulverize, or incinerate by burning the device in a licensed, or organizationally approved and validated incinerator.

**SECTION 1 - DATA DISPOSITION**

- I am closing the entire DUA and all associated files. I am only closing certain files on the DUA but leaving the DUA open.
- I am destroying the physical media but leaving the DUA and all files open.
- Other – Must be preapproved by CMS. Provide preapproved language below.



