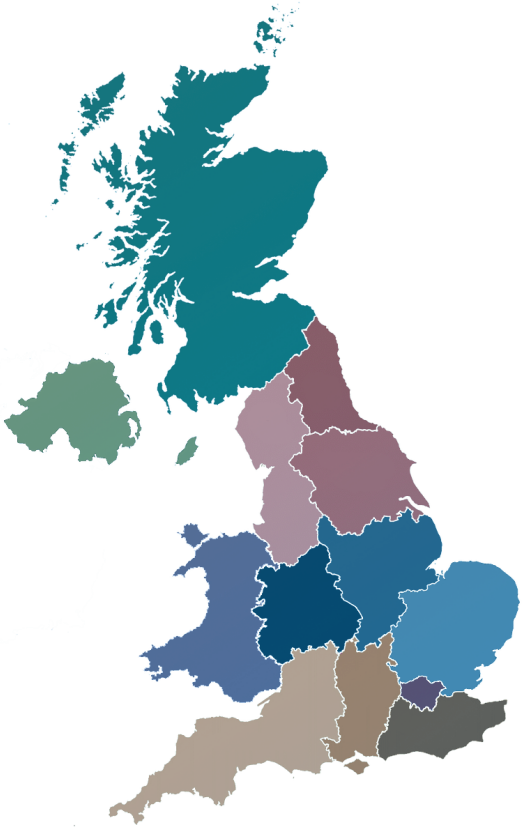
UK National Health Service: Data Sanitisation Guidelines For N3 Connected Networks

The National Health Service in the UK recently made major changes to their data sanitisation guidelines. These guidelines were published in the *Destruction and Disposal of Sensitive Data: Good Practice Guidelines* and *Sanitisation, Reuse, Disposal and Destruction of Electronic Media: Guidance For Health and Care Organisations* policy updates. The updated guidelines provide recommendations for the secure erasure of patient data on many different types of media.



DATA REMOVAL AND DESTRUCTION RECOMMENDATION

The NHS guideline provided many recommendations for the effective management of data destruction:

- At a minimum, ensure the hard disk serial numbers are tracked for audits.
- Use inventory tracking software when cost effective.
- Log all media that contains sensitive information. Must include type of media and end of use date.
- Log all destruction and removal certificates by the actor destroying and the date.

WHICH MEDIA DEVICES NEED DATA REMOVAL?

The NHS guidelines state that data removal should be performed on:

- Flash disk drives and USB
- Solid state disk drives (SSD)
- Digital recorders
- Hard disk drives (HDD)
- Mobile Telephones
- Photocopiers
- Cameras

These devices must have a multi-pass overwrite pattern performed onsite before the IT assets leave the organization or are reallocated. The NHS guidelines recommend Data Clearing or Data Purging for data removal on these assets. These two options are different in the methodology and use case.

DATA CLEARING

If a data-bearing device is going to be used in the same environment with the same security levels then Data Clearing can be used on that device. For example, if a laptop is being reassigned to another doctor in the same office, then a Data Clear is sufficient to meet the data removal guidelines.

Data Clearing must be performed by a commercially sourced and licensed data sanitisation tool – no free or open source tools. The Secure Erase (SE) ATA command must be used on the devices. If the drive is not compatible with the SE command then the drive can be wiped with the "HMG Infosec Standard #5 - Enhanced" multi-pass overwrite pattern. Any SSD's that are not compatible with the SE command must be destroyed. The software deletion tool can be performed by non-specialist staff or approved contractors.

DATA PURGING

When a data-bearing device moves to a new security level then the data on the drive must meet "NIST 800-88" Purge level classification. All other requirements from the Data Clearing guidelines must be met as well.

To ensure all data has been removed, a third party must verify that no data is left on the drive. A report of this verification must be archived.

NHS GUIDELINES ARE MET BY WIPEDRIVE ENTERPRISE

WipeDrive Enterprise is a commercially available and certified tool for the removal of data from NVMe, SSD and hard disk drives. WipeDrive provides the "NIST 800-88r1" overwrite pattern which will attempt to reach Clear or Purge classification level of sanitisation. The overwriting process is simple and easy to start for any staff member or contractor. The tamper-proof reports are available without a Console or other management system and WhiteCanyon Software provides a separate verification tool that can be used on other erasure programs.

WHY USE WIPEDRIVE ENTERPRISE?

- WipeDrive Enterprise's "NIST 800-88r1" overwrite pattern is Common Criteria and NCSC certified and meets NHS's Data Removal guidelines.
- WipeDrive Enterprise has submitted itself for approval by the G-Cloud (approved list of NHS service providers).
- WipeDrive Enterprise provides award-winning Customer Support in the UK

WipeDrive Enterprise is the preferred vendor of data erasure tools in the UK and EU.

Contact our Sales Team at +44 203.808.5120 for more information on NHS Data Removal.