Destruction and Disposal of Sensitive Data

Good Practice Guidelines

Version: 3.2

Date: January 2017

Contents

1. Introduction

This guide addresses the major security issues associated with the destruction and disposal of any media that has contained information relating to sensitive data, or has operated within an N3 connected network. It aims to establish vendor and product independent guidelines to assist organisation in minimising the risks of data disclosure through inappropriate deletion of data, or inadequate destruction of media prior to disposal.

This document includes guidance on ensuring the confidentiality and integrity of sensitive information. It includes:

- An overview of data media types
- An overview of safely removing data from media and guidance on the safe destruction of media
- An overview of safely disposing of written or printed information on non-electronic media

1.2 Aims and Objectives

The following information provides a knowledge-based framework that will help maintain best practice values in your own organisation. In using this guide, you will be conforming to best practice and therefore avoid some of the consequences of non-compliance.

After reading this document you should understand:

- The minimum standards for the secure deletion of sensitive data from systems used within N3 connected networks, which could be regarded as live or active systems
- Methods and standards of correct disposal and certification of media which may have contained sensitive data or which have operated within N3 connected networks
- Methods and standards of correct disposal and certification of written or printed media which may have contained sensitive data

1.3 Assumed Reader Knowledge

This document assumes a general familiarity with the requirement to protect patient sensitive data at all times, with a general understanding of computing related terms.

Further information on information security and related matters is available from the Health and Social Care Information Centre's Infrastructure Security Team at http://systems.hscic.gov.uk/infogov/security/infrasec (N3 connection required).

2. Background

Information disclosure has become a major risk to organisation working with sensitive data, primarily due to the increasing dependence on electronic storage systems and the use of disposable media.

NHS and third party systems may deal with patient identifiable, business critical or sensitive data. To prevent unauthorised disclosure it is essential that assured data destruction take place.

This document offers guidance on the security measures requiring consideration when removing data from live systems or when decommissioning systems, while allowing the organisation to conform to the NHS Information Governance Statement of Compliance[1].

There have been numerous published disclosures of sensitive information through seemingly benign channels such as the purchase of second hand hard disk drives through online auction websites. These disclosures occur due to inappropriate deletion of information on the target media leaving historical data vulnerable to retrieval through various widely available methods.

3. Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NHS Digital or Health and Social Care Information Centre (HSCIC). The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

Any party relying on or using any information contained in this document and/or relying on or using any system implemented based upon information contained in this document should do so only after performing a risk assessment. It is important to note that a risk assessment is a prerequisite for the design of effective security countermeasures. A correctly completed risk assessment enables an NHS organisation to demonstrate that a methodical process has been undertaken which can adequately describe the rationale behind any decisions made. Risk assessments should include the potential impact to live services of implementing changes.

This means that changes implemented following this guidance are done so at the implementer's risk. Misuse or inappropriate use of this information can only be the responsibility of the implementer.

[1] http://systems.hscic.gov.uk/infogov/igsoc

4. Overview of Data Media Types

The following table lists common media types in use at the time of publication of this document. It is not an exhaustive list of all possible media types, but instead offers a representative sample of the most common forms of media currently in use. These media types also demonstrate the characteristics that determine the appropriate deletion or destruction methods required to assure data is non-retrievable. All multi pass pattern wiping deletions should be via a commercially sourced and licenced product. Open Source or Freeware is not an acceptable solution.

Table 1: Media and Data Destruction methods

Media Type	Data Storage Mechanism	Suggested Removal Methods
Hard Disk Drives (HDD)	Non-volatile magnetic	Multi Pass Pattern wiping, disintegration or incineration
Solid State Disk Drives (SSD)	Non-volatile solid state memory	Multi Pass Pattern wiping, disintegration
CD-R / DVD-R	Write once optical	Abrasion, disintegration, incineration
CD-RW / DVD-RW	Write many optical	Abrasion, disintegration, incineration
BD-R	Write once optical	Abrasion, disintegration, incineration
BD-RE	Write many optical	Abrasion, disintegration, incineration
Ultra-Density Optical (UDO)	Write once or write many optical	Abrasion, disintegration, incineration
Magnetic Tape	Non-volatile magnetic	Degaussing, disintegration, incineration
Flash Disk Drives and USB	Non-volatile solid state memory	Multi Pass Pattern wiping, Degaussing, disintegration
Paper based	Printed	Micro Cross Cust Shredding, incineration
X-Ray Film	Photographic film	Shredding, metal recovery

5. Non Volatile Magnetic: Hard Disk Drives

Hard disk drives are extremely popular and are widely used as the primary storage medium for the majority of desktop PCs and laptops. Physically, they can be extremely small whilst simultaneously providing large amounts of storage space. The storage medium usually consists of a glass platter with a magnetic substrate. Data remains even after removal of power from the drive.

5.1 Data Removal and Disposal Methods for Hard Disk Drives

Hard Disk Drives can be securely erased and redeployed within an organisation to promote reuse of IT equipment. If a HDD is to be reused in an environment or system with equivalent security controls to that where the HDD was previously used, the clearing process must be applied. For HDDs which will move to a less secure environment or may leave the organisation for resale or disposal, the purging process must be applied. Refer to Section 8 for information on the methods that should be used to securely erase information from HDDs.

Where HDD equipment is rendered inoperable by electronic or physical failure, the destruction processes described in this document must be used. This may require the use of a specialist computer disposal contractor, who should conform to the BSEN15713:2009 standard and must be multi pass pattern wiped onsite.

Organisations should pay particular attention to manufacturer warranty or swap-out programme, where system vendors provide onsite engineers to exchange faulty hardware for new replacements. Some manufacturers may offer provide written assurance that media will be handled securely and destroyed following testing, which should be obtained by an organisation prior to releasing faulty hardware which has held sensitive data. If this is not available, faulty hardware which has held sensitive data should be multi pass pattern wiped and destroyed in accordance with the processes described in this document. In all instances, a certificate of destruction must be provided.

6. Optical Media

Optical Media can be broadly categorised into two groups write once and write many times. Disposable media such as CDs and DVDs are cheap to purchase but cannot be reused once written to, in comparison rewritable media is more expensive but often lasts for many rerecording cycles.

Other types of optical media are available for intensive use or long term archiving requirements, with greater reliability but an increased media cost.

6.1 Write Once Optical: CD R, DVD R, BD R

CD-Rs, DVD-Rs and BD-Rs consist of a plastic platter with an optical substrate applied. A focused laser beam writes the data by burning the substrate in an encoded pattern which can then be read by any drive that supports the chosen recording format.

6.2 Write Many Optical: CD RW, DVD RW and BD RE

Although similar to write once media, write many media uses a light sensitive dye to record the data instead. Laser light changes the state of this dye; this allows the rewriting of the media. Data may not be written sequentially, which means that a disc can be erased for reuse and written to, but not added to overtime. There are exceptions to this process such an open disc session but this data type is not portable between systems.

6.3 Write Many Optical: Ultra Density Optical (UDO)

A UDO disc is a 5.25 cartridge-type optical disc capable of storing up to 60 GB of data. It is designed for heavy duty or extended use environments, and is a popular format to archive bulk data for long term storage and later retrieval. UDO is faster and cheaper to implement than its predecessor, Magneto-Optical (MO) technology. Both write-once read many (WORM) and rewritable media are available.

6.4 Data Removal and Disposal Methods for Optical Media

Rewritable optical media can be erased and reused through the use of erase functions available in disc recording software. Most software packages use a quick erase function which clears the header sections of the disc but does not remove all files. This means that it may be possible to recover information from an erased disc, and therefore this method should only be used when a disc is to be reused in an environment of equivalent security to that where the disc was last used. If this type of reuse is not possible the disc should be destroyed.

Most common types of optical disc media are of a write once type and thus cannot be reused. Physical destruction is the most appropriate method for disposal. Refer to Section 9 for information on appropriate methods.

7. Solid State Storage

7.1 Solid State Disk Drives

Solid State Disk Drives (SSDs) are gaining in popularity over Hard Disk Drives (HDDs) for use in high-performance applications. This is primarily due to their fast data seek times in comparison to HDDs. SSDs use NAND flash memory to read and write data as opposed to the iron-oxide coated glass platters and moving electromagnetic heads used in HDDs. SSDs do not contain any moving parts which makes them preferable for low-energy consumption applications. Various logical mechanisms are in use to extend the lifetime of SSD media and prevent errors, which can improve device reliability but make data removal processes challenging.

7.2 Solid State Portable Storage

Solid-state portable storage devices usually consist of integrated circuits embedded in a plastic substrate, such as SD memory cards and USB memory sticks. The storage of sensitive information on this type of media is not advisable because of their small size and portability, and therefore corresponding risk of loss.

Organisations can choose to store sensitive information on removable media following a risk assessment and the introduction of enhanced controls such as encryption and password based or biometric authentication or remote wiping applications.

7.3 Paper Based Information

Despite the growth of electronic storage, paper based records are still in extensive use. This category may also include other hybrid methods of storage such as microfiche, card and specialist record storage material. All documents containing PID must be micro cross cut shredded to at least HMG S5 Infosec DIN Level 4/5 onsite prior to disposal.

X-ray film is still in regular usage across the NHS and other third-party healthcare providers. Many film types contain silver halide which can be recovered by specialist waste treatment contractors, allowing reuse of the material and decreasing environmental contamination.

8. Data Removal Techniques

Many of the methods described in the following sections will be applicable to various different media types. It is recommended that specific removal methods are discussed with suitable vendors or contractors in line with the information provided in this guide. All multi pass pattern wiping deletions should be via a commercially sourced and licenced product. Open Source or Freeware is not an acceptable solution.

8.1 Classification of Data Removal

There are two major data removal classifications that help determine the methods used as well as the possible costs involved. Data Clearing offers a fast method of data destruction using software applications but is only suitable for use on media which is to be redeployed in an environment of equivalent security controls to that of where the media was last used. Data Purging is a more thorough method of data destruction, and is used when media moves from an existing security zone to a new security zone. This new security zone may or may not be more secure than the current security measures in effect.

8.2 Clearing

If the disk drives/media will remain within the same environment in which they are currently situated (and existing security measures will continue to cover them), the most appropriate removal method is clearing.

Clearing involves simpler removal methods. As long as particular sections of data need removing and comprehensive data removal from the media is not required, then non-specialist staff or approved contractors may carry out clearing.

Most ATA-type Hard Disk Drives manufactured after 2001 include the Secure Erase command within the drive firmware, which allows an administrator to quickly and effectively clear data from the drive. This process requires the installation of application software on the host system that can execute the Secure Erase command on the hard disk drive.

The Secure Erase command is also capable of overwriting reallocated disk sectors, where the drive has moved data due to hard errors. This provides an advantage over the use of data clearing software programs, which cannot erase bad disk sectors.

For hard disk drives which do not offer Secure Erase support, software applications are available which perform sequential writes of patterned data, ensuring that data is not easily recovered using standard techniques and programs.

The clearing of data must be to HMG Infosec S5 Multi Pass pattern wipe (minimum of 3 passes) minimum.

All multi pass pattern wiping deletions should be via a commercially sourced and licenced product.

Open Source or Freeware is not an acceptable solution.

8.3 Purging

Purging is required when media moves from an existing security zone to a new security zone. This new zone may or may not be more secure than the current security measures in effect.

After removal of media from its current security context there must be sufficient care taken to ensure that data is irretrievable, even if specialised recovery methods are used (e.g. platter scanning or the use of electron microscopes).

For systems which support the Secure Erase command, the clearing process is technically equivalent to the purging process. Verification testing performed by CMRR shows that the erasure security is at the Purge level of NIST 800-88, because drives having the command also randomise user bits before storing on magnetic media.

The Full Disk Encryption Enhanced Secure Erase (FDE-SE) process proposes an enhancement to existing Secure Erase processes by changing the encryption key of the hard disk drive thus rendering any encrypted data on the drive inaccessible. It should be noted that FDE SE encryption is not yet tested for protection against advanced forensic analysis, and is presented here for information purposes. The use of a Secure Erase process following the use of FDE-SE would ensure the destruction of data for environments where this level of assurance is required.

8.4 Data Removal from Live Systems

There are various scenarios in which data may need removing from a system while still in operation, or reuse of the media is required for financial or policy reasons.

In these cases, organisations should make all possible efforts to remove the required data from the target media while not adversely affecting the performance of live systems or the long-term effectiveness of the media to perform the role required of it. In this case, the most common scenario would be to remove the data from hard disks or tape backup devices using processes built into applications or operating systems when a particular application no longer requires it. A Certificate of Destruction will be required.

8.5 Data Removal for Media Reuse

Often media such as hard disk drives are reused rather than being completely decommissioned. It is the reuse requirement, therefore, that should be the driving force behind the removal methods used (following the guidance above regarding clearing and purging).

3 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

In many infrastructure environments, hard disk reuse is common. A particular disk may be reused across many different individual machines or business uses. In this scenario, clearing is a sufficient method of ensuring data is non-recoverable. Keeping a log of all clearing processes (for each disk drive) provides an audit trail that records all the areas that the disk has been in use and, before reuse of the disk in a different area, the verification of data removal.

Best practice instructs that unless there is a compelling business reason to do so, media should not transfer between differing securities contexts.

If media does require moving between security contexts, purging needs conducting in line with the guidance in this document to ensure that no data is retrievable, by multi pass pattern wiping (minimum of 3 passes) to HMG Infosec S5 Enhanced.

All multi pass pattern wiping deletions should be via a commercially sourced and licenced product. Open Source or Freeware are not an acceptable solution.

Maintaining a log (including certificates of verification for each individual media device and information regarding the new use of the disk) is extremely useful for audit as it ensures the media is traceable even after it has left its original security context.

8.6 Verification of Data Removal

If a specialist company or contractor has processed the media, there should be a procedure for verification of data removal, including the issuing of certificates.

If local staff have carried out the data removal then the process should be recorded with the verification results and stored with all other relevant documentation.

Tools that attempt to retrieve data from media which has undergone a data removal process can be extremely useful in verifying that complete data removal has taken place.

If any files or fragments of files are evident, then data removal has been unsuccessful. If so, repeat the process using a greater number of passes or consider using a different technique altogether.

9. Media Destruction Techniques

Media which is no longer required or has passed its effective reuse period should be destroyed according to the processes below, or passed to a specialist contractor for secure disposal. Organisations should ensure that where local data destruction and disposal is conducted, the methods within this document are followed and any waste products are disposed of in accordance with the Waste Electrical and Electronic Equipment (WEEE) regulations[4]. Local contractors are available in most areas that are able to provide this service.

Where organisations choose to outsource the responsibility of data destruction and media disposal, the selected contractor should conform to the BS EN 15713:2009 standard. This sets out requirements for how sensitive information is collected, retained and transferred, the processes and standards for destruction, and the security measures for premises and personnel. Many of the techniques described for the destruction of media can involve dangerous substances or exposure to possibly toxic particulate matter, so can often require specially controlled environments and waste treatment processes. In all instances data wiping must occur prior to removal from site.

9.1 Hard Disk Destruction

Due to the current costs of storage, large arrays of hard disks are utilised in preference to other backup methods, such as tape or optical storage. This is due to the speed and ease of retrieval and the added resilience of data when mirrored across many hard disk drives.

Degaussing is a simple method that permanently destroys all data and disables the hard disk drive. Degaussing uses a high-powered magnetic field that permanently destroys data on the disk platters. It also renders the drive hardware components inoperable, requiring manufacturer intervention to replace critical parts.

The recommended specification for data destruction is the SEAP 8100 and HMG Infosec S5 Enhanced standards used for classified government material. Equipment that complies with this standard assures complete data destruction.

Degaussing is generally safer for organisations to conduct than physical destruction processes and subject to the use of appropriate techniques the destruction of data is total and permanent. Degaussing equipment can be obtained by organisations and safely operated when following manufacturer instructions. Degaussed drives can then be disposed of as standard electronic waste which must be in accordance with the Waste Electrical and Electronic Equipment (WEEE) regulations. Local contractors are available in most areas that are able to provide this service. In all instances a certificate of destruction will be required.

[4] https://www.gov.uk/government/publications/weee-regulations-2013-government-guidance-notes

Due to the component makeup of disk drives, only a specialist company in a secured and environmentally isolated location should undertake hard disk destruction. All casing materials must be removed and the disk platters disintegrated, to ensure the removal of all magnetic material. A disposal certificate must be obtained to document the destruction of hardware which contained sensitive data. In any event Disk Drives must be multi pass pattern wiped to at least HMG S5 Enhanced (min 3 passes) on site prior to disposal.

9.2 CD, DVD and Blu ray Disc Destruction

The construction of plastic media such as CDs and DVDs makes them particularly vulnerable to damage if handled roughly. Most optical media consists of a plastic base with a laser sensitive substrate applied to one side.

Optical media can be destroyed through the use of shredding machines that separate the disc into small pieces. All shredding machines must produce parts of no greater than 4mm x 15mm micro cross-cut to destroy sensitive data.

Other optical media destruction systems are available, for example grinding machines which use a rotary handle attached to an abrasive pad to grind away the recording surface. These machines are very effective but expensive, and are therefore only likely to be cost-effective when disposing of large volumes of optical media. The discs should then be disposed through waste recycling processes.

Optical discs are made from Polycarbonate (No. 7 plastic) which often cannot be recycled using local authority waste collection processes. Polycarbonate is a reusable material and chips can be reused to manufacture new items such as automotive parts, building materials, and safety equipment. Organisations should contact local plastic recycling companies in their area to recycle this material rather than sending it to landfill.

9.3 Solid State Device Destruction

Solid state devices include SSDs, Flash-based USB drives and memory storage cards for personal digital assistants (PDAs) and other handheld devices. Due to the compact nature of their internal makeup, the complete physical destruction of the device is required to ensure that any recovery of data is impossible.

Disintegration and incineration are the most effective techniques for disposal of solid-state storage. Disintegration processes must break devices into pieces small enough to ensure that printed circuit boards and integrated component parts are adequately destroyed. Guidance can be found in EN15713:2009[5] which specifies cutting sizes based on the size of the original device. Incineration processes will melt both the plastic casing and the internal circuitry of small components such as SD cards. This ensures that it is not possible to reuse or recover any aspect of the internal storage mechanism. Incineration processes should only be undertaken by specialist electronic waste disposal contractors.

Devices such as USB flash drives should be physically destroyed using disintegration methods. In most cases a specialist contractor would be the most

[5] http://www.bsia.co.uk/Portals/4/Publications/form_204_id_en15713.pdf

appropriate choice to destroy these devices, however organisations can undertake the disintegration process if required, where appropriate facilities exist. The outer casing must be removed and the internal circuitry must be broken into tiny fragments, including any integrated component parts which can be cut or drilled to render them inoperable. Any plastic components should be recycled using local waste recycling facilities.

If a solid state storage device has previously contained sensitive data, it must be multi pass pattern wiped on site to HMG Infosec S5 Enhanced which should be carried out by a specialist contractor service on site and certificates obtained.

9.4 Magnetic Tape Backup

Magnetic tape formats vary significantly in their suitability for reuse and available clearing techniques. Some forms of magnetic tape can be degaussed and successfully reused as blank media. However some advanced tape formats rely on servo tracking data to record information on a blank tape, which is removed by the degaussing process and therefore makes this method unsuitable. Organisations should consult their hardware vendor for information on which system types will allow reuse of degaussed media.

The most effective method for the destruction of magnetic tape is the disintegration or shredding of the tape media. Various processes exist to disintegrate both the magnetic tape and the protective cartridge, with the possibility to recover and recycle the waste plastics produced.

Organisations should note that modern tape formats such as LTO Ultrium also contain EEPROM (electrically erasable programmable read-only memory). microchips which record potentially identifiable data such as tape library information, usage, and volume contents. Use of this storage mechanism is controlled by the backup management application. These types of tape cartridges must be disposed of by specialist computer waste disposal contractors, who conform to the BS EN 15713:2009 standard.

9.5 Paper Based

Traditionally, paper based disposal has consisted of simple vertical shredding. However this method is not suitable for sensitive or confidential information.

The HMG Information Assurance Standard (IS5) requires the shredding of paper records be conducted using a micro cross cut shredder that cuts the paper into pieces of no more than 15mm x 4mm. This standard is in line with the requirements of BS EN 15713:2009 and is therefore recommended for the destruction of sensitive information. This must be conducted on site prior to disposal or removal.

Incineration processes may also be used in addition of the above to dispose of paper records and other types of printed media. A certificate of destruction from a specialist waste disposal contractor is required on completion.

10. Management of the Data Removal and Destruction Process

It is important to maintain an effective method of managing the process of data destruction. This ensures that all media requiring cleaning or destruction is correctly stored, organised and properly accounted for. The use of a data removal and destruction process also helps to achieve successful audit results by demonstrating repeatable steps and records of media which was processed.

It is recommended that a log of all media is kept that may contain sensitive information. This should detail the specification of the media and its effective end of use date.

Use of inventory tracking software may be helpful in limiting the administration overhead in larger organisations. Tracking of hard disk serial numbers should be used as a minimum control for individual component tracking where other methods are not available.

The log should also contain a section for destruction or removal certificates; these provide evidence guaranteeing the destruction or sanitisation of the media by the nominated waste disposal contractor and the date on which the destruction occurred.