

	Disposal and Destruction of Sensitive Data			
	Programme	<i>NPFIT</i>	DOCUMENT RECORD ID KEY	
	Sub-Prog / Project	<i>Information Governance</i>	<i>NPFIT-FNT-TO-IG-GPG-0008.01</i>	
	Prog. Director	<i>Mark Ferrar</i>		
	Owner	<i>Tim Davis</i>	Version	<i>1.0</i>
	Author	<i>James Wood</i>		
	Version Date	<i>31/03/2006</i>	Status	<i>APPROVED</i>

Disposal and Destruction of Sensitive Data:

Good Practice Guidelines

Amendment History:

Version	Date	Amendment History
0.1		First draft for comment
0.2	24/8/2005	Comments Integrated into Second Draft
0.3	15/02/2005	Technical Author
0.4	31/03/2006	Approved

Forecast Changes:

Anticipated Change	When
Annual Review	March 2007

Reviewers:

This document must be reviewed by the following. Indicate any delegation for sign off.

Name	Signature	Title / Responsibility	Date	Version
Malcolm McKeating		IG Security Team Manager		1.0
Tim Davis		Head of Information Governance		1.0

Approvals:

This document requires the following approvals:

Name	Signature	Title / Responsibility	Date	Version
Mark Ferrar		Director of Technical Infrastructure		1.0
Tim Davis		Head of Information Governance		1.0

Distribution:**Information Governance website:**

<http://nww.connectingforhealth.nhs.uk/>

Document Status:

This is a controlled document.

This document version is only valid at the time it is retrieved from controlled filestore, after which a new approved version will replace it.

On receipt of a new issue, please destroy all previous issues (unless a specified earlier issue is baselined for use throughout the programme).

Related Documents:

Ref no	Doc Reference Number	Title	Version
1	NPFIT-SHR-QMS-PRP-0015	Glossary of Terms Consolidated.doc	12

Contents

1	Introduction	5
	Abstract.....	5
1.1	Aims and Objectives	5
1.2	Assumed Reader Knowledge	5
1.3	Background	6
1.4	Disclaimer	6
2	Overview of Data Media Types.....	7
2.1	Non-Volatile Magnetic: Hard Disk Drives	7
2.2	Write Once Optical: CDROM and DVD-R	7
2.3	Write Many Optical: CD-RW and DVD-RW	7
2.4	Solid State.....	8
2.5	Paper Based	8
3	Removal of Data	8
3.1	Classification of Data Removal	8
3.2	Data Removal from Live Systems	9
3.3	Data Removal for Media Reuse	9
3.4	Verification of Data Removal.....	10
4	Media Destruction Techniques	10
4.1	Hard Disk Destruction	11
4.2	CD-ROM and DVD Destruction.....	11
4.3	Solid State Devices	11
4.4	Magnetic Tape Backup.....	12
4.5	Paper Based	12
5	Data Removal and Destruction Management	12
5.1	Media Log	13

1 Introduction

Abstract

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

You will find guidance on ensuring the confidentiality and integrity of sensitive information. This includes:

- An overview of data media types.
- An overview of safely removing data from media and guidance on the safe destruction of media.

1.1 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 completing this guide, 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 and which has operated within N3 connected networks.

1.2 Assumed Reader Knowledge

- A general familiarity with the requirement to protect patient sensitive data at all times.

Further information on network security and related matters is available from the NHS Connecting for Health Information Governance website:

<http://nww.connectingforhealth.nhs.uk/igsecurity/>

1.3 Background

Due to the increasing dependence on electronic storage systems and the use of disposable media, data disclosure has become a major risk in the operation and decommissioning of media.

- N3 connected 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 decommissioning systems), while allowing the organisation to conform to the NHS Connecting for Health Code for Digital Services.
- There have been numerous disclosures of sensitive information through seemingly benign channels such as purchasing second hand hard drives through online shopping 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.

1.4 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 Connecting for Health. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. NHS Connecting for Health shall also accept no responsibility for any errors or omissions contained within this document. In particular, NHS Connecting for Health shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

2 Overview of Data Media Types

The following table (Table One) 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.

Media Type	Data Storage Mechanism	Suggested Removal Methods
Hard Disk Drives	Non volatile magnetic	Pattern wiping, Incineration
CDROM/DVD-R	Write once optical	Abrasion, Incineration
CD-RW/DVD-RW	Write many optical	Abrasion, Incineration
Magnetic Tape	Non volatile magnetic	Degaussing, Incineration
Flash Disk Drives	Solid state	Pattern wiping, Physical destruction
Paper Based	-	Shredding, Incineration

Table One: Media and Data Destruction Methods

2.1 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 while 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.

2.2 Write Once Optical: CDROM and DVD-R

CDROMs and DVD-Rs consist of a plastic platter with an optical substrate applied; a focused laser beam writes the data by 'burning' the substrate.

2.3 Write Many Optical: CD-RW and DVD-RW

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 (although data may not be written sequentially). Due to its low financial cost, destruction is the preferred method of disposal.

2.4 Solid-State

Solid-state devices usually consist of integrated circuits embedded in a plastic substrate, such as SD memory cards. Storing sensitive information on this type of media is not advisable because of their small size and corresponding ease of loss.

2.5 Paper Based

Despite the growth of electronic storage, paper based records are still in extensive use. This category may also include other 'physical' methods of storage such as microfiche, card and specialist record storage material.

3 Removal of Data

Many of the methods described in the following sections will be applicable to various different media types. We recommend discussing specific removal methods with vendors/contractors in line with the information provided in this guide.

3.1 Classification of Data Removal

There are two major data removal classifications that help determine the methods used as well as the possible costs involved:

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 contractors may carry out clearing.

Typical clearing programs use sequential writes of patterned data, ensuring that data is not easily recovered using standard techniques and programs. The pattern matching should involve at least three writes of data. The following is a typical example:

1 st write	01101100
2 nd write	10010011
3 rd write	00101110

This method attempts to mask any previous data with two sets of data that are a mirror of each other, thus 'blanking' previous data on the disk. A random set of data is utilised to fill all available space with meaningless information.

To ensure that historical data is thoroughly removed it is advisable to make as many passes as is practicable.

The likelihood of total data eradication is proportional to the amount of passes.

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 methods are used (e.g. platter scanning or the use of electron microscopes).

Purging involves the use of more sophisticated tools and therefore requires specialist personnel working within a controlled environment.

Advise contractors that purging of the media is required. A minimum of seven passes qualifies as a purging process.

(See http://www.dss.mil/isec/nispom_0195.htm for further information on avoiding unauthorised disclosure of sensitive information).

3.2 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, 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, when a particular application no longer requires it.

3.3 Data Removal for Media Reuse

Often, media such as hard disk drives are reused rather than 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).

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 security contexts. If media does require moving between security contexts, purging needs conducting in line with the guidance (above) to ensure that no data is retrievable, using any means.

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

3.4 Verification of Data Removal

Once 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 (along 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.

4 Media Destruction Techniques

Media, which is no longer required (or has passed its effective reuse period), should be passed to a specialist contractor for secure disposal. Many of the techniques described for the destruction of media can involve dangerous substances or exposure to possibly toxic particulate matter, so often require specially controlled environments.

4.1 Hard Disk Destruction

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

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

The recommended specification for data destruction is the SEAP 8500 Type II standard used for classified government material. Equipment that complies with this standard assures complete data destruction.

Degaussing is generally safer than physical destruction and (assuming the contractors use the appropriate techniques) the destruction of data is total and permanent.

The most permanent method is the complete physical destruction of the drive and its platters. Due to the component makeup of disk drives, only a specialist company (in a secured and environmentally isolated location) should carry this out. All casing materials need removing, and the disk platters sanding, to ensure the removal of all magnetic material, prior to the destruction of the platter itself.

4.2 CD-ROM and DVD Destruction

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

Achieving permanent destruction removing this substrate with a machine such as a belt sander may release toxic particulate matter into the atmosphere. It is therefore necessary for professional destruction companies to undertake this type of destruction.

Breaking the plastic base into small fragments, and disposing of the remains as normal waste, is suitable for non-sensitive data. Some paper shredding machines now support destruction of CDs in this manner; follow the manufacturer's instructions carefully to ensure proper destruction and personal safety.

4.3 Solid-State Devices

Solid-state devices normally consist of Flash USB drives or memory storage cards for 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.

Incineration 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 any aspect of the internal storage mechanism.

Devices such as USB thumb drives should be physically destroyed using brute force methods. As long as appropriate safety methods are in use, non-specialist staff can destroy these devices. The outer casing requires removal and the internal circuitry needs breaking into tiny fragments (including any integrated circuit chips).

If the device has previously contained sensitive data destruction should be carried out by specialist services and certificates obtained.

4.4 Magnetic Tape Backup

The most effective method for the destruction of magnetic tape is the disintegration or shredding of the tape media. Physical destruction should take place after the tape is appropriately degaussed.

4.5 Paper Based

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

The UK Security Service (MI5) recommends shredding of paper records be conducted using a cross cut shredder that cuts the paper into pieces of no more than 15mm x 4mm.

For further information see <http://www.mi5.gov.uk/output/Page56.html>.

Incineration may also be used. However, a certificate of destruction from a specialist contractor is required on completion.

5 Data Removal and Destruction Management

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 organised and properly audited.

5.1 Media Log

We recommend keeping a log of all media 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 a bare minimum for individual component tracking.

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