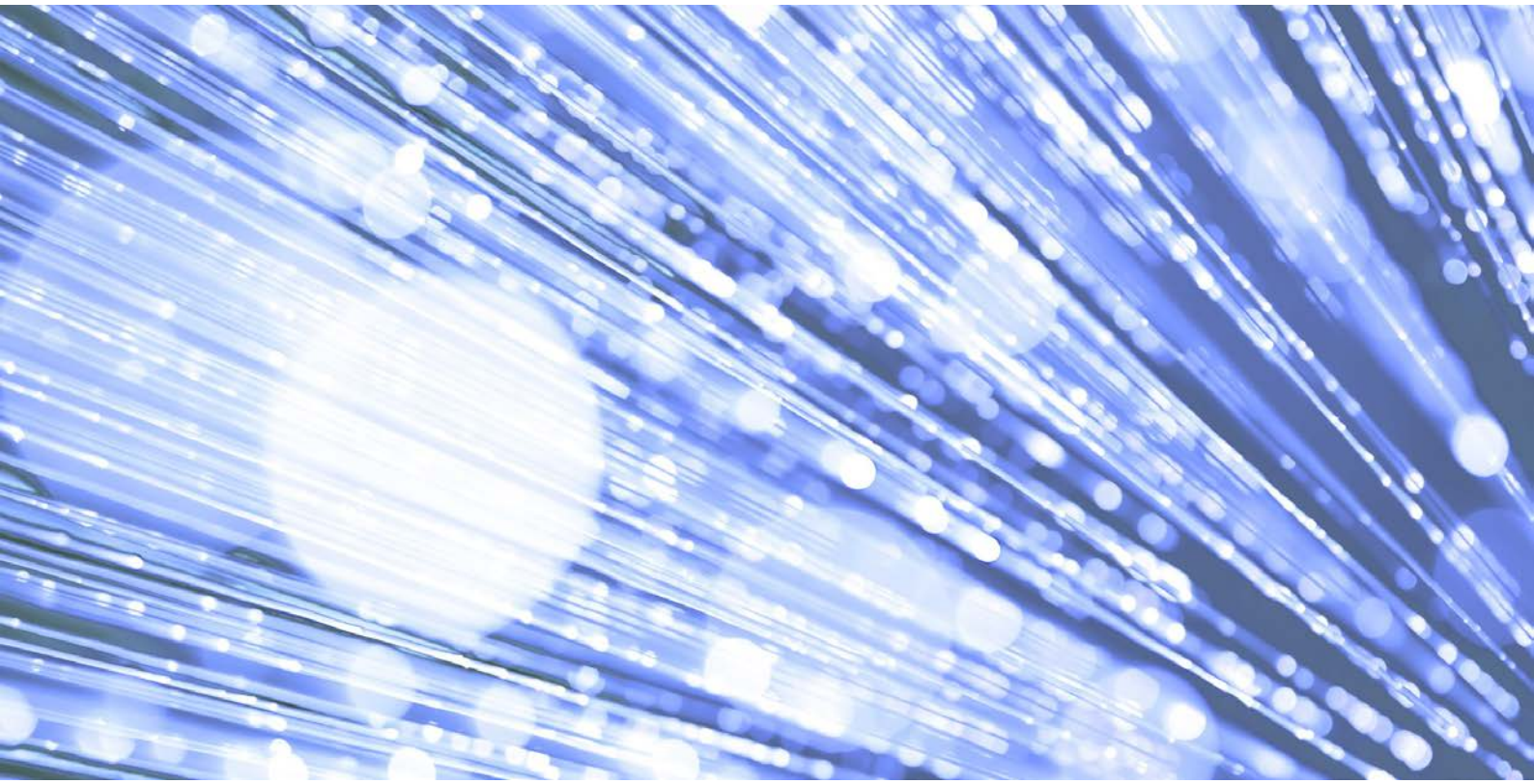
Sanitisation, Reuse, Disposal and Destruction

Good Practice Guide

Author: A Heathcote
Date: 22/05/2017
Version: 1.0



Information and technology
for better health and care

Contents

1 Purpose

The purpose of this Sanitisation, Reuse, Disposal and Destruction Good Practice Guide (GPG) is to provide guidance on how an organisation should implement an organisation wide, robust and fit for purpose system for the sanitisation, reuse, disposal and destruction of IT and electronic media.

This guidance will enable organisations to have procedures and processes in place that will enable them to:

- Successfully and appropriately sanitise electronic media according to the sensitivity and/or classification of data on it.
- Successfully and securely reuse electronic media without putting data at risk of being breached.
- Successfully and appropriately dispose and destroy electronic media according to the sensitivity and/or classification of the data stored on it.

2 Scope

This Sanitisation, Reuse, Disposal and Destruction GPG relates to all electronic media that store or process NHS and other UK Government information in electronic form utilised by and NHS and health and social care (large or small).

3 Applicability

This Sanitisation, Reuse, Disposal and Destruction GPG is applicable to and designed for use by any NHS, health and social care or associated organisations that use or have access to NHS systems and/or information at any level.

4 Guidance

This Sanitisation, Reuse, Disposal and Destruction GPG supplements the Example Policy on producing a Sanitisation, Reuse, Disposal and Destruction Policy and provides greater detail on how the policy requirements can be achieved. It is not prescriptive and it is realised that different organisations will require different levels of management. This GPG provides the minimum that should be considered. The guidance provided should be scaled according to the size of the organisation. This GPG will:

- Outline the general principles
- Outline the methodologies for sanitisation and disposal/destruction.
- Summarise what sanitisation is and when it should be considered.
- Summarise the type of electronic media that need to be considered and where data may be stored.
- Outline the process for determining when sanitisation and/or destruction may be required.
    - Reuse within a similar environment.
    - Reuse in a different environment.

- Describe (briefly) the types of sanitisation and destruction methods for media types that may be required – full details should be taken from the latest HMG or industry best practice.
- Outline management processes for media awaiting sanitisation, reuse or disposal/destruction.
- Outline the considerations for maintenance and disposal by third parties of electronic media.
- Capture the most likely regulatory requirements.

4.1 General

- The Sanitisation, Reuse, Disposal and Destruction of electronic media is critical for the protection of data/information. The requirements for the sanitisation, reuse, disposal and destruction of media is different depending upon 2 main factors:
  - The classification and/or sensitivity of the data/information on the media.
  - The type of media – e.g. hard disk drive, flash media, CD, etc.
- To enable the processes and procedures for the sanitisation, reuse, disposal and destruction of electronic media to protect the data the following should be undertaken:
  - Identification of the highest classification and/or sensitivity of data stored on the media.
  - Identification of the type of media.
  - Identification of what is intended to be done with the media – i.e. reuse within the organisation and which environment this is to be in, passing of the media to third party for maintenance or repair or final disposal/destruction of the media.
- At all times of the decision making process for the sanitisation, reuse or destruction of the media the impact to the NHS and/or social care should be the underlying core requirement with respect to:
  - The confidentiality of the data on the media – i.e. maintain its confidentiality.
  - The reputation of the organisation for protecting and managing classified and/or sensitive data appropriately.
- This GPG provides guidance and, where applicable, examples on implementing appropriate and authorised sanitisation, reuse or destruction methods when re-using or disposing of electronic media to ensure that that the data cannot be reconstructed, recovered or retrieved and made available to persons who do not have a 'need to know' or should not have access to the data.
- Where the sanitisation and destruction/disposal requirements relate to information above OFFICIAL-SENSITIVE or NHS CONFIDENTIAL (i.e. SECRET or higher) then the requirements of Information Assurance Standard No 5 – Secure Sanitisation and NCSC requirements **must** be followed and met. The processes in this GPG should be followed but the minimum criteria from NCSC/CESG must be followed. It is, however, unlikely that NHS and social care organisations will process data at SECRET.

4.2 Sanitisation, Disposal and Destruction Methodologies

- The type of sanitisation, disposal and destruction methods deployed should follow best practice. There are a variety of means for achieving sanitisation and destruction of media but it is recommended that the organisation follows HMG best practice. This can be found at:
  - https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media - guidelines.
  - https://www.ncsc.gov.uk/document/security-characteristics-data-sanitisation - approved technologies and providers for data sanitisation and destruction.
  - Within the archived CESG Information Assurance Standard No 5 – Secure Sanitisation Issue 5 dated April 2014.

4.3 What is Sanitisation and When Should it be Considered for Use?

- Sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow the re-use of the media, while others are destructive in nature and render the media unusable.
- The use of sanitisation of media should be considered when the organisation:
  - Wants to allocate a device to a different user or repurpose some equipment – reuse. This includes wanting to re-sell unwanted equipment so that it can be re-used elsewhere.
  - Wants to return a faulty device to the vendor for repair or replacement.
  - Wants to dispose of the media but it has sensitive data on it – the organisation may wish to sanitise unwanted media before it is passed outside of the organisation – especially if there is limited confidence in the third party contracted to dispose of it on the organisation's behalf.
  - Wants to destroy the media – this may be on site or through a third party. If it is via a third party, sanitisation of the media first may be prudent if there is limited confidence in the third party provider.

4.4 What are the Risks of Not Sanitising?

- If the media is not sanitised appropriately this could result in:
  - Unknown whereabouts of sensitive or classified data.
  - Loss of control over the organisation's information assets.
  - Critical data recovered and used by adversaries or the media for reputational impact.
  - Private or personal data about patients or staff used to commit fraud or identity theft or blackmail.
  - Loss of reputation.

4.5 Encryption – Is this a Sanitisation Process?

- It is important to note that encryption of media is not usually accepted as a sanitisation method; it is a mechanism for protecting data on the media whilst in use.

As the data is not removed it is not truly a sanitisation process. However, in some circumstances it may be used for re-use of equipment. (This is covered later in the GPG.)

4.6 Types of Electronic Storage Media and their Data Storage Capability

- A wide range of electronic storage media may be used to store or process information. A number of these, with some data storage facts, are summarised below:
  - Desktop computers - the data is not just stored in the Hard Disk Drive (HDD) or Solid State Drive (SSD) but some data retention is possible within Random Accessible Memory (RAM), Erasable Programmable Read-Only Memory (EPROM) and Field-Programmable Gate Array (FPGA).
  - Servers – these can store extensive amounts of data – Hundreds or thousands of terabytes or even petabytes. An average laptop or desktop has ½ terabyte for data storage to give a comparison.
  - Multifunction devices (e.g. printers) – these often have data storage devices – either as SSDs or 'flash' media. (Flash is a solid-state non-volatile computer storage medium.)
  - Photocopiers – as with multifunction printers these also store data using electronic media.
  - Laptops, tablet computers and electronic notebooks – are very similar to desktops in that they have HDDs or SSDs plus RAM, EPROMs and FPGAs.
  - Mobile telephones – modern smartphones are capable of storing considerable volumes of data on flash type memory devices.
  - Digital recorders – these often have storage devices or can take SD cards (secure digital card – a type of flash memory) to store data.
  - Cameras – these can store data either within the storage media (SSD/flash) inherent in the device or by the insertion of memory devices such as SD cards.
  - USB devices – such as pen drives; these can hold considerable amounts of data (anything from 8 to 64 gigabytes (GB) or more.
  - DVDs, CDs and other portable devices and removable media such as SD cards.

4.7 Reuse of Electronic Media

- It is good practice, and financially more efficient, to reuse electronic media as much as possible as these items can be expensive. However, before any electronic media can be reused the risks of its reuse should be assessed to ensure the data's confidentiality is not being put to an unacceptable risk of compromise. This assessment basically asks 2 questions:
  - Is the media to be used within a similar environment? This fundamentally ascertains whether the data to be stored and processed in the new environment will have the same (or very similar) classification and/or sensitivity as the data that it stored in the previous environment.
  - Is the media to be used in a less secure or lower classification/sensitivity environment? This fundamentally ascertains whether the data to be processed will

be the same/similar or of a lower classification/ sensitivity that it had previously stored/processed.

- The answers to these 2 questions will determine the type of sanitisation method that will need to be deployed, or whether sanitisation is possible and the media can (or cannot) be reused.
- If sanitisation is identified as being required then:
  - The sanitisation technology will depend on the type of media and the environment/classification that it is to be re-used in; and
  - The sanitisation method must irretrievably destroy any data held on the electronic media.
  - If this is not possible then the media must be destroyed.

4.7.1 Environment and Data Classification/Sensitivity Assessment

- In the assessment of the data and environment it is important that the classification and/or sensitivity is carefully examined. Below are some examples to illustrate this point:
  - Is the information/data currently stored on the media to be at the same or a different HMG classification as that in the new environment?
    - If the current environment is for OFFICIAL is the new environment also OFFICIAL with no additional security markings such as SENSITIVE?
    - If the current environment is for OFFICIAL-SENSITIVE is the new environment also for OFFICIAL-SENSITIVE and is it the same type of SENSITIVE data (e.g. financial or personal or patient data) or is it different? It may have additional descriptors such as PERSONAL or COMMERCIAL.
  - Is the information/data currently stored on the media to be at the same NHS sensitivity/classification as that in the new environment?
    - If the current environment has stored data at NHS PROTECT will the new environment also be for NHS PROTECT?
    - If the current environment has stored data at NHS CONFIDENTIAL will the new environment also be for NHS CONFIDENTIAL and if so is it the same type of sensitive data – i.e. is it personal data, financial data, patient medical information, etc.
- In addition to assessing the data it is also important that the actual environments are compared. This comparison should evaluate:
  - Physical security of the environments – similar or different control of entry mechanisms to the offices and server rooms, and similar or different security measures on the desktops, laptops and server racks?
  - Personnel security of the environments – are the clearance and vetting requirements of the staff similar or different, and are the numbers of personnel accessing the environment similar or different?
  - Technical security – are similar or different technical security measures in forces; such as encryption of laptops, password mechanisms for user log-ons, ability to have or not have remote access and anti-virus/malware protection mechanisms, including use of intruder detection or prevention services?

4.7.2 Reuse Within the Same or Equivalent Secure Environment

- If the assessment of the data and environment has determined that the data/information is the same **and** that the environment security characteristics provide a comparable level of security **and** there are no 'need to know'constraints, then the media may be re-used without any sanitisation. However, the existing data must be deleted before being re-used. If the data cannot be deleted then the media should be sanitised.

4.7.3 Reuse Within a Less Secure Environment

- If the electronic media is to be re-used to store data of a lower classification or sensitivity **or** be operated within a less secure environment, then the media must be appropriately sanitised. If sanitisation is not possible then the media should be destroyed.

4.8 Sanitisation and Destruction Methods for Media Types

- This GPG does not contain the full list of HMG approved or Industry Best Practice for data sanitisation and media destruction requirements as there is a vast range of media types and the policy/best practice change on a regular basis. The latest HMG guidance can be found from the CESG archived Information Assurance Standard No 5 – Secure Sanitisation Issue 5 dated April 2014 and from the NCSC website (https://www.ncsc.gov.uk/document/security-characteristics-data-sanitisation), which lists approved methodologies/providers for data sanitisation.
- The below table contains some examples of the types of media and methods that may be used for data sanitisation and destruction.

Device Type & Data Classification	Environment Criteria	Sanitisation/Destruction Requirement
HDD containing OFFICIAL-SENSITIVE data.	To be used within the same environment and for data of the same classification/sensitivity.	Overwrite the entire storage space with random/garbage data and verify that only that data can be read back.
HDD containing OFFICIAL-SENSITIVE data.	To be used within a less secure environment or process data of a lower classification/sensitivity.	Apply a destructive procedure to the platter that prevents it from turning. Data sanitisation is not possible.
SDD containing OFFICIAL data.	To be used within the same environment and for data of the same classification/sensitivity.	Use the secure erase command to write zeroes over the entire data area.
SDD containing OFFICIAL data.	To be used within a less secure environment or process data of a lower classification/sensitivity.	This is one occasion when encryption can be utilised due to the unique nature of SSD data writing. Removing and destroying the encryption key will render the original content of the SSD unreadable

Device Type & Data Classification	Environment Criteria	Sanitisation/Destruction Requirement
		(assuming contemporary industry-standard encryption is used), allowing re-use in different (or less secure) environments.
Blu-Ray Disc (BD), Compact Disc (CD) and Digital Versatile Disk (DVD) containing NHS CONFIDENTIAL.	To be used within the same environment and for data of the same classification/sensitivity.	For re-writable discs only, use a standard BD, CD or DVD erase function (not available for BD-ROM, BD-R, CD-ROM, CD-R, DVD-ROM, DVD-R and DVD+R discs).
Blu-Ray Disc (BD), Compact Disc (CD) and Digital Versatile Disk (DVD) containing NHS CONFIDENTIAL.	To be used within a less secure environment or process data of a lower classification/sensitivity.	Shred or disintegrate using equipment that meets a recognised international destruction standard. Particles should be no larger than 6mm in any direction. Data sanitisation is not possible.

4.9 Electronic Media Awaiting Sanitisation, Reuse or Disposal

- All electronic media awaiting disposal retains the classification/sensitivity of the data it holds until it has been sanitised or destroyed using an approved mechanism. Therefore, all media must be stored and handled securely in accordance with the requirements for its classification and/or sensitivity.

4.10 Maintenance and Disposal by Third Parties

- It is likely that many organisations (large and small) will make use of third parties for either the provision of their IT or at least its maintenance and repair. Organisations will need to be assured that the sanitisation and disposal of electronic media by third parties is in accordance with the organisation's policy and guidance in this GPG. It is recommended that this GPG and the associated NCSC/HMG guidance (listed under **Purpose** and under **Further Reading and Advice**) is used to assist in drawing up and managing contracts with third party providers.
- As a core baseline the below approach is recommended for third party providers:
  - Faulty or unserviceable electronic media appropriately sanitised in accordance with the latest HMG mandatory requirements before being removed for repair, replacement or disposal.
  - All leased electronic media sanitised in accordance with the latest HMG mandatory requirements before being returned to the vendor.

- All electronic media that is maintained or disposed of by third parties handled appropriately as required for its classification so that there is no risk to the confidentiality of the data stored.

4.11 Record of Reuse and Destruction

- It is recommended as good practice that the sanitisation and destruction undertaken on any media is recorded and related to the asset number of the electronic media concerned. This approach is also recommended in the NHS GPG for Information Asset Management.

4.12 Legal and Regulatory Requirements

- There will be legislative and regulatory impacts to data sanitisation and particularly for media destruction. As a minimum, the Secure Sanitisation and Disposal mechanisms will be impacted by the following Acts and Regulations:
  - Data Protection Act 1998 – relating to the protection of personal data.
  - Caldicott Data Guardian Principles and Data Security Standards – relating to handling of personal confidential information.
  - EU Waste Electrical and Electronic Equipment (WEEE) Directive and the UK Waste Electrical and Electronic Equipment Regulations 2006 – relating to the disposal of electronic equipment.
- Where other legislation or regulations affect the organisation and these impact upon data/information handling they should be included in any decision making processes.

4.13 Incident Reporting

- It is also important to note that any release or re-use of electronic media without appropriate sanitisation should be considered to be an information security incident and should be reported in accordance with the organisation's Information Security Incident Policy and Procedures.

5 Further Reading and Advice

- In addition to the documents listed under Related References, Links and Documents further details and advice on secure sanitisation and destruction can be found at https://www.ncsc.gov.uk/. This GPG does not list the particular references as these change on a frequent basis, however, searches under the below headings will help to locate the current applicable HMG policy and standard or an assured provider or mechanism of the technique or technology that may be required:
  - Data Sanitisation.
  - Media Disposal.
  - Secure Sanitisation.
  - Secure Disposal.
- This GPG is supported by other GPGs, which should be used in tandem. This includes, but is not limited to:
  - Sanitisation, Reuse, Disposal and Destruction
  - Information Security Incident Policy

- Asset Management.
- Encryption

6 Key Words

Destruction, Disposal, Electronic Media, Encryption, Reuse, Secure Sanitisation