NHS Information Governance:

Information Risk Management

Guidance: Maintenance and Secure Disposal of Digital Printers, Copiers and Multi Function Devices

Department of Health Informatics Directorate

July 2010

Amendment History

Version	Date	Amendment History
1.0		First published version

Introduction

This Information Governance (IG) guidance provides NHS organisations with a general awareness of the associated risks for maintenance and disposal of digital printers, copiers and multifunction devices.

Terms used:

Digital Printers enable printing using digital techniques developed for computer printers such as inkjet or laser printers.

Digital Copiers use similar digital techniques to printers and may be used to scan images and store or archive documents.

Multi Function Devices (MFD) may include printing, scanning, copying, fax and other inbuilt functions that may potentially be accessed and used across digital networks.

Why are Digital Printers, Copiers and MFDs an Information Governance issue?

These devices share much of their technology with computers and operate by scanning documents into onboard electronic memory before printing. A particular IG concern is that scanned documents or images copied to the storage disc or electronic memory of the device before printing may be permanently retained even when no longer required.

Such devices also present additional risks. Maintenance staff or support staff may need to connect a laptop or other diagnostic device and this may create the opportunity for sensitive or confidential data to be extracted or copied to any network that the laptop or diagnostic device is subsequently connected.

Most manufacturers incorporate erasure and encryption technologies within their products to help protect data, but not always. Some care is necessary as these measures may not have been independently evaluated, verified and assured, or indeed the functionality available may be set to a default ‘off’ state.

What can be done to minimise the risks?

NHS organisations should always undertake and document a formal local information risk assessment whenever such digital devices are to be procured or leased and deployed. This is particularly important in scenarios where patient or other sensitive or confidential information is likely to be involved. Risk Assessment will help the Information Asset Owner (IAO) responsible to identify likely threats and the potential controls necessary. The assessment should include security, technical and support issues. In addition, consideration will be necessary of the equipment provider’s claims for inbuilt security measures including data erasure and encryption capabilities where provided.

Avoiding problems through guidance and countermeasures

Security controls should be considered to minimise the risk of unauthorised disclosures of both NHS patient information and other sensitive or confidential NHS data. These controls should significantly reduce the possibility of any potential confidentiality breach, be that of protectively marked information or otherwise sensitive data that may be stored on these devices.

Possible controls that may apply include:

- Liaison with the equipment providers to:

  - Identity the most up to date and reliable sources of guidance for their devices;

  - Determine appropriate fault reporting processes and procedures;

  - Agree appropriate on-site authorisation and oversight procedures before service/maintenance staff may access premises where the device is located

- Service/maintenance staff may be required to enter NHS premises in order to service or repair the device. Therefore, it is important that the organisation's Information Governance (IG) policy and procedures cover this type of on-site support arrangement. These should include procedures to control the introduction or removal of magnetic storage media or other components by visiting service/maintenance staff. Equally should the device or its parts need to be removed for offsite repair or replacement there is a risk that any information stored could still be accessed, particularly where faults have prevented use of the device's information purge/destroy functions (i.e. scenarios requiring replacement of the hard disk).

- The organisation should also consider the need for controls that prevent "/control" remote access for maintenance, support, updating or any other purpose.

- Procedures should exist for data sanitisation (where possible) or destruction of any unserviceable component, in particular electrostatic drums, hard disks and memory components.

- Hard disks that need to be replaced should be securely purged or destroyed. This will include memory technologies & Semi-conductor (SC) chips: - These devices contain a range of memory types that could retain sensitive information for a considerable period of time.

- The NHS organisation's IG policy and security processes for the disposal or reuse of these devices should not differ from those applied to a PC or Server etc. However, in the case of a networked MFD or photocopier it is recommended that organisations adopt a worst case scenario approach by considering the highest protective marking or information sensitivity the device could have stored/handled during its lifetime (not just the current business area) and apply relevant purge or destroy processes.

- Temporary provision of a controlled laptop loaded with the necessary commercial diagnostic software for use by visiting service/maintenance staff.

- Copiers/MFDs should be sited in supervised environments or in separate rooms where access may be controlled.

- To prevent unauthorised use, photocopying equipment should be locked or disabled when not required,and any device access keys or tokens held by authorised users and stored securely when not needed..

- Security Architecture: MFDs need to have a network interface; ideally they should be connected to networks that provide them with some defence to unauthorised use or attack.

- Contractual aspects: To further ensure NHS organisations may satisfy their NHS IG responsibilities, local IG policies and standards for data sanitisation/reuse, the specific processes (hard disk removal, purging etc) should be clearly referenced within any contracts for the purchase or leasing and support of these types of devices. Contractors should also provide details of any relevant implications for device warranties etc.

- General review of organisational IG policies should be undertaken to address the acceptable use of digital printers, copiers and other multifunction devices. Organisational IG policies and standards should be clear about the acceptability of forwarding information from an organisation's intranet connected device. The consequences of non-compliance with organisational IG policy should also be clear.

Whilst there are a number of technical and procedural controls that can be applied to block or control permitted usage, a major defence against the threats associated with maintenance and disposal of digital printers, copiers and multifunction devices is first and foremost an awareness of the risk issues. It is therefore extremely important that the issues and applicable controls are identified through information governance risk assessment processes that inform local policies and procedures. These in turn should be both appropriately communicated and made accessible to staff and contractors involved in support and maintenance activities.