



NEWCASTLE-UPON-TYNE HOSPITALS NHS TRUST.

OFF SITE & DATA TRANSFER POLICY

| | |
|-------------------------|---------------------------------|
| PROJECT NAME | Data Transfer & Storage |
| DOCUMENT TITLE | Off Site & Data Transfer Policy |
| DOCUMENT VERSION | Vers. 1.0 |
| RELEASE DATE | November 2003 |
| DOCUMENT OWNER | IM&T |
| REVIEW DATE. | November 2006 |

**Data Transfer Policy
Confidential**

Contents

DOCUMENT HISTORY.....3

DISTRIBUTION LIST.....3

INTRODUCTION.....4

MANAGEMENT.....4

DATA PROTECTION ACT.....4

TECHNICAL.....6

SUMMARY.....6

ANNEX A Data Transfer Form.....7

ANNEX B Extract from NHSIA Sysop 2002.....8

Data Transfer Policy
Confidential

| Version | Release Date | Amendment Summary |
|----------------|---------------------|-------------------------------|
| Draft Ver 1.0 | May, 2002 | Draft version for discussion. |
| Draft Ver 1.1 | Jan 2003 | Updated after BS7799 review. |

| Name | Role | Department |
|-----------------------|-----------------------|--------------------|
| IM&T Group | Document Owner | Corporate |
| Internal Audit | Audit | Audit |
| Richard Oliver | Author | IT Security |

Data Transfer Policy Confidential

INTRODUCTION

This Policy is in line with the Trust Information Policy and IM&T Security Policy and provides guidelines for the management and use of Trust information and equipment outside the Trust.

Equipment and data will not be taken off site without formal signed approval, other than to transport it from one of the Trust's sites to another.

Portable equipment is very vulnerable to theft, loss or unauthorised access. Strong security measures should be introduced as soon as practicable after purchase, particularly if such equipment has networked access capability.

To preserve the integrity of data, frequent transfers should be made to the Trust network servers.

Managers and Users should be aware that whilst this policy refers directly to personal data, corporate or business information may be sensitive when aggregated together and should be considered for protection in the same way as personal data.

Managers and Users will comply with the following guidance on the practical implementation of the Policy.

Personal portable devices not owned by the Trust ie; Laptops and PDAs (Personal Digital Assistant) MUST NOT be connected either directly or indirectly to the Trust network. Without the knowledge and consent of the IT Department.

MANAGEMENT

1. Managers must maintain a list of ALL staff who send or take personal data off-site, which is normally kept on systems in the Trust.
2. Users must be aware that they are responsible for the security of the data they are taking away, whether on a laptop PC, hand-held device or on removable media (e.g. floppy disk/CD/tape).
3. A Data Transfer Form will be completed for all instances of data being taken or transmitted off-site. An example is attached at Annex A. If the transfer involves a non-NHS third party then a Third Party Agreement should also be completed. On Completion the form should be returned to the IT security team.
4. Specific guidance will be prepared for staff wishing to work at home on systems not owned by the Trust, particularly with regard to access controls and virus protection software.

Data Transfer Policy
Confidential

DATA PROTECTION ACT

5. If data copied from Trust systems is to be used for a different Purpose¹ than registered, the Caldicott Guardian & Data Protection officer must be informed.
6. If the person taking the data off-site is going to use it legitimately for his/her own purposes (e.g. a Consultant who has a Private Practice), then the individual MUST register separately with the Data Protection Commissioner, and comply with the Procedures and Principles of the Data Protection Act.

TECHNICAL

7. Laptop computers are able to hold as much sensitive personal data as desktop PCs. Users should assess the risks of taking data with them to meetings or to work on at home. Particular care should be taken during transportation to prevent systems being stolen from vehicles or by leaving items unattended, even momentarily.
8. At the very least, users should password protect individual files as they are saved to disk, using their application. This should happen whether the files are saved to the internal hard disk of a portable PC or temporary storage such as a floppy disk or 'zip' drives.
9. If the system is normally networked within the Trust, then strong authentication must be implemented if the system is to be used by dialling in to the Trust network from outside. See separate guidance on External Access to Trust Networks. At present, authentication is effected with the use of SecureIT , a 'smart card' which provides a frequently changing numeric password that is synchronised to the system within the Trust. This card must not be kept with the system.
10. The standard method of marking portable systems as Trust property (Trust asset tag) must be rigorously enforced, as this may be the only way of proving ownership of the hardware if the data is password protected or encrypted and therefore not readable.
11. A back-up copy of the data must be maintained on systems within the Trust, and updated as soon as practicable whenever the data on the portable system is changed.
12. PDA. The Trust does not supply PDAs as standard. The use of personally owned PDAs must be registered with the IT Department.
13. Trust data held on PDAs is subject to the same conditions as all other methods of data transfer. A sensitive data transfer form must be completed and the PDA owner must register the use of data with the Caldicott Guardian

¹ It may be that the Purposes of Use registered by the Trust were, for example, Health Administration and Services. If the data were being taken off-site for the purpose of Research, then the Data User (the Clinician responsible for the collection and use of the data) would need to change the internal registration and begin to inform all new Data Subjects of the new Purpose before he could authorise its removal and use. If data already collected is involved, then 'Positive Consent' may be required from individual Data Subjects, particularly if identifiable Personal Data is being used.

Data Transfer Policy
Confidential

14. Technical advice and guidance should be sought in the first instance from the IT Helpdesk on 25954. Problems relating to personnel and procedures should be raised with the IT Security Officer or Data Protection Officer.

SUMMARY

The use of portable/laptop/hand-held computers is becoming increasingly popular, and the likelihood of systems being stolen or magnetic media being lost becomes greater. Issues regarding the risk of access by unauthorised persons or propagation of software viruses must also be addressed.

Management and users must ensure that they minimise these risks and provide adequate technical and procedural protection against loss or disclosure.

Annex A Sensitive Data Transfer Form

**Data Transfer Policy
Confidential**

SENSITIVE DATA TRANSFER FORM

| DATA TRANSFERRED FROM: | DATA TRANSFERRED TO: <small>(if non-NHS 3rd party, agreement attached)</small> |
|--|---|
| NAME | |
| ADDRESS | |
| PURPOSE/REASON for TRANSFER | |
| DATA TYPE e.g. patient, staff, business/finance | |
| DATA DESCRIPTION | |
| DATABASE(S) USED e.g. PAS, Pathology, Radiology | |
| PHYSICAL TRANSFER METHOD e.g. Floppy, Tape, Network, NHSNet, Portable PC | |
| SOFTWARE FORMAT USED e.g. Word, Excel, CSV, etc. | |
| ENCRYPTED or UNENCRYPTED | |
| DATE and TIME OF TRANSFER or commencement if ongoing | |
| FREQUENCY IF ONGOING | |

I the undersigned certify that the personal data being received will not be disclosed to unauthorised persons. The Data and their Purposes of Use are registered under the Data Protection Act 1998 and my organisation/company is committed to compliance with the Data Protection Principles.

| | |
|------------------|--|
| DATE | |
| SIGNATURE | |

Data Transfer Policy
Confidential

JOB TITLE

| |
|--|
| |
| |

Annex B.

Extract from NHSIA Sysops 2002 published 26th Sept.

2. General Risk Management Principles

2.1 Using a PDA involves Risk Management. (BS7799-2:2002 Clause 4.2.1) If NHS User Organisations were to adopt a Risk Avoidance strategy then PDAs could not be used at all. Organisations and Users have to accept that there are some risks and occasionally breaches, compromises and incidents will happen. Should the rate of occurrence of such breaches compromises and incidents rise to an unacceptable level then local policies derived from this document, and this document itself, must be reviewed.

2.2 Individual users or groups of users should not make unilateral decisions, based on this document, on using PDAs for NHS business purposes. They must follow the Security Policy and Operating Instructions issued by their organisations. (BS7799-2: 2002 Annex A 3.1) **They must note that, as with fully connected IT systems, it is not acceptable to use PERSONAL IT equipment for the storage or processing of Patient Identifiable or other NHS sensitive data or for such equipment to be connected to any NHSnet connected system.**

2.3 PLEASE COMPLETE THIS FORM AND RETURN TO:

| |
|---|
| <p>IT SECURITY OFFICER IT DEPARTMENT ROYAL VICTORIA INFIRMARY QUEEN VICTORIA ROAD NEWCASTLE-UPON-TYNE NE1 4LP</p> |
|---|