Pennine Care NHS
NHS Foundation Trust

Policy Document Control Page

Title:
Title: Protocol for the Management of the Removal / Transfer of Records and Information Storage Equipment when Moving Premises / Location

Version: 5

Reference Number: CO62

Keywords:
Records, case notes, mental health, community, IT, moving, removals, equipment, accommodation, log, confidentiality agreement, service request form

Supersedes: Version 4
Description of Amendment(s):

- **No significant changes**

Important Notice
From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.

Originator
Originated By: Carole McCarthy
Designation: Records Manager

Equality Analysis Assessment (EAA) Process
Equality Relevance Assessment Undertaken by: Carole McCarthy
ERA undertaken on: 04/01/2016
ERA approved by EIA Work group on:

Where policy deemed relevant to equality-
EIA undertaken by
EIA undertaken on
EIA approved by EIA work group on

Approval

Referred for approval by: Carole McCarthy

Date of Referral: 21st January 2016

Approved by: Information Governance Assurance Group

Approval Date: 27th January 2016

Date Ratified by Executive Directors: N/A

Executive Director Lead: Medical Director

Circulation

Issue Date: 11th February 2016

Circulated by: Performance and Information

Issued to: An e-copy of this protocol is sent to all wards and departments

Protocol to be uploaded to the Trust's External Website? YES

Review

Review Date: January 2018

Responsibility of: Carole McCarthy

Designation: Records Manager

This protocol is to be disseminated to all relevant staff.

This protocol must be posted on the Intranet.

Date Posted: 11th February 2016

1. INTRODUCTION

1.1 Everyone in Pennine Care NHS Foundation Trust has a duty of care to ensure that all records, and especially confidential records, are stored in a safe and secure environment, which recognises their sensitivity.

1.2 This procedure specifically addresses the procedures to be adopted when premises (or parts of premises) cease to be used for their current purpose, and are vacated by the individuals, teams, or organisation currently using them.

1.3 Pennine Care NHS Foundation Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records can easily go missing during office moves and this exposes the organisation to unnecessary and avoidable risks.

1.4 This procedure relates to all sensitive paper records both corporate and clinical (see 2.1.2)

1.5 All electronic records should be stored on secure network drives, please adhere to the Computer Use Policy.

1.6 This procedure document should be read in conjunction with the Trust's Records Management Policy, which is available on the Pennine Care NHS Foundation Trust Intranet (CO20)

2. PREPARING FOR A MOVE OF ACCOMMODATION OR PREMISES

2.1.1 A risk assessment should be undertaken prior to any move of the records storage facility in the new premises for security, suitability, size and adequacy.

2.1.2 It is the responsibility of the Service / Departmental Manager to organise a departmental move.

2.1.3 When preparing for a move, the Service/ Departmental Manager (or a nominated deputy) should identify:

- All clinical and other service user records (all presumed to be sensitive and confidential) ;

- All other records which include person identifiable data (eg staff records, payroll and employment records, recruitment files, notes associated with complaints - all presumed to be sensitive and confidential); and
- All other administrative records (some of which might also be sensitive or confidential in nature) e.g. copy correspondence, budget reports, copy requisitions etc
- All computers and mobile devices (e.g lap tops, tablets, CDs and Memory sticks)

- Any notice boards/charts/leaflets with person identifiable information

A log should be produced scheduling all of the records that are sensitive or confidential and noting their location (e.g. Filing cabinet in room x), together with all of the computers and other data storage devices (Appendix 1)

Against each entry in the log, the intended destination of the items should be noted (including where the record is planned for disposal) along with the officer responsible for receiving them at the new site.

2.2 It is good practice to appraise the documents and records prior to any move in order to minimise the cost and time taken with transporting superfluous records. In culling old records reference should be made to the Records Management Policy on retention of records. Pennine Care NHS Foundation Trust has adopted the retention periods set out in the Records Management: NHS Code of Practice available on the intranet in the **Guidance for the retention of all clinical and corporate records**. (see Section 4)

2.3 Where contractors are assisting with the moves, they should be made aware of the presence of sensitive records and their written procedures obtained identifying how they will safeguard them during transit. They must also sign a confidentiality agreement (Appendix 2)

2.4 Cupboards and cabinets that are moved with records ‘in-situ’ should be locked and clearly marked with the content, whether it is sensitive data, and its destination. The key for these cabinets/ cupboards should not travel with the item of furniture but with a designated staff member.

2.5 Other records should be packaged into boxes, which should be clearly marked with the content, whether it is sensitive data, and its destination. If using crates for the transfer of confidential documents, these should be sealed with a cable tie prior to removal and only opened by a designated member of staff at its final destination.

If contractors are undertaking the packing, they should be supervised on-site by a member of staff at all times who is familiar with the records being packed, and who can 'sign-off' that the packing is complete and appropriate.

2.6 The IT department should be informed of the date of the move and a service request made so that they can safely unplug the equipment and ensure it is safely and securely packaged and also they will need to be present when the equipment is unloaded in the new premises. (Appendix 3)

2.7 Note – the Service /Departmental manager, or nominated deputy, must be someone who is familiar with the contents of the records being moved, and aware of the risks and sensitivities involved with the particular records in question.

3. MANAGING THE ACTUAL MOVE

3.1 The service / departmental manager or nominated deputy is responsible for:

- Ensuring the security of all information and records being moved.
- Accurately labeling the boxes and making sure that they are securely fastened.
- Compiling a list of all boxes containing sensitive or confidential records and signing off in conjunction with contractors assisting with the move.
- Being present to oversee sensitive records being moved out of the offices, or premises.
- Informing the IT Department in advance of the date of the move (see Appendix 3)
- Carrying out a thorough inspection of the premises, or relevant part of the premises, to ensure that all packages, records, and other items, have been collected and moved. The inspection should include the rooms, the corridors, reception areas, storage units and cupboards and the area used for loading. This inspection should be undertaken with

the contractor in attendance and both parties should formally sign-off that all items (paying especial attention to sensitive records) have been removed.

- Being present to oversee sensitive records being moved into the new offices, or premises. For audit purposes, the written log should identify that all packages logged out at the old site, are logged into the new site. Delivery vehicles should be checked to see that nothing has been left in the vehicle.

4. DESTRUCTION OF RECORDS

4.1 (See 2.2)

4.2 When clinical records are destroyed a record should be kept of the service user's name, a description of the record and the date the record was destroyed. This list of destroyed records should be retained permanently and held securely within the department. This should also be reflected, if tracked on NCRS.

4.3 If sensitive records are being disposed of via a contractor, the contractor must provide a certificate of their safe and complete disposal. A brief description should be kept of everything that has been destroyed, when, and by whom. A template is available (see Appendix 4).

5. FINAL INSPECTION OF VACATED PREMISES

5.1 Where premises are being vacated, it is important that, once the move has taken place, the service manager, or nominated deputy, revisits the vacated premises to ensure that no residual records or other Pennine Care items are left on the premises (including notice boards)

5.2 If the building is being sold/ demolished or no longer the responsibility of Pennine Care then a mini task force comprising of a representative(s) from the Estates Department, Health & Safety and the Records Manager should make a final check of the building before any keys are handed over to the new landlord (if appropriate).

5.3 For audit purposes the outcome of this visit should be recorded, signed / dated and retained by the Estates Department.

6. DONATING OR DISPOSING OF UNWANTED STORAGE FURNITURE

The Department donating or disposing of an item of furniture that could house confidential records are responsible for ensuring that the item of furniture has been emptied of all Trust records prior to the item of furniture being removed from the premises.

7. STORAGE OF RECORDS WHEN SERVICES HAVE BEEN DISBANDED OR TRANSFERRED TO A NEW PROVIDER

7.1 Consideration needs to be given to the storage of records when a service is to be disbanded or transferred to a new provider. This must form part of the business transfer agreement when considering options by the Trust. For advice please contact the Trust's Records Manager

7.2 Consideration also needs to be given as to whom will continue to be responsible for the records once the service has been disbanded or transferred to a new provider e.g. subject access request requiring authorisation.

8. REVIEW

8.1 This procedure will be reviewed every two years by the Information Governance and Estates Team (or sooner if new legislation, codes of practice or national standards are to be introduced).

8.2 This procedure will be approved by the Information Asset Owners and Information Asset Administrators prior to ratification by the Trust Executive Director's.

Appendix 1

Pennine Care NHS
NHS Foundation Trust

Log of Information Storage Equipment / Transfer of Records
(to be used when moving premises / location)

Name of Department……..Date of Move:……..

Service /Departmental Manager……..

List of Records / Information Storage Equipment	Location	New Location

Appendix 2

Confidentiality Agreement

Actions:

1. Send two copies of the agreement to the third party for signature

2. On return, send both copies to the Caldicott Guardian for signature

3. The department head will sign both copies, send one to the third party for their records, keep one copy, which should be photocopied and sent to the Information Governance Manager so that a central register of all agreements can be kept.

Pennine Care NHS
NHS Foundation Trust

Confidentiality Agreement

1. Introduction

The Data Protection Act and other legislation relating to information security bring a number of changes and, in particular, impose certain obligations on users of information. It is important that adequate security measures are in place to ensure that the information is only used for the purpose for which it has been provided and that there is no unlawful disclosure or loss of the same.

For the Trust's compliance with legislation, the Trust has developed this confidentiality agreement. A party (hereinafter called "the Requestor") must sign and comply with this Agreement in order to obtain access to personal information held by the Trust.

This Agreement should only be used where there is no existing contract between the parties that already adequately deals with the matter of personal information confidentiality.

This Agreement shall come into effect on the last of the dates below the signatories of the Trust and the Requestor. However it may apply retrospectively to any relationship between these parties if a date is included hereafter:

This Agreement shall apply retrospectively from the date of

…… [delete if not applicable]

2. Information sharing

2.1 The Requestor may request certain personal information relating to individuals and other information (images, research, finance). However, the use of information must be in accordance with the terms of this agreement.

3. Code of confidentiality

The Requestor undertakes that it:

3.1 Shall maintain the information received in strict confidence and shall not forward the information or a copy of it, in whole or in part, to a third party except in the case where it is necessary for the Requestor to perform any

obligation(s) owed to the Trust or which arise under statute **and where the third party:**

(a) is or will be contracted to the Requestor; and

(b) requires the said information in order to perform the said contract; and

(c) has first signed a copy of this Confidentiality Agreement direct with the Trust.

3.2 Shall not make use of or otherwise process the information other than for the strict purposes as agreed with the Trust.

3.3 Shall restrict access to the information solely to its responsible employees and/or the aforesaid third party's employees who need to have such access to it for the purposes agreed with the Trust.

3.4 Acknowledge the Trust's and service users' legal rights in the information received and that the disclosure to a third party of any information shall not confer upon the third party any rights whatsoever in respect of any part of such information, **except for the purposes expressly agreed as between the third party and the Trust.**

3.5 Shall take only those copies of any document or other material necessary for the purposes as agreed with the Trust. The Requestor shall immediately on request by the Trust return any information together with any copies or extracts taken by the Requestor. The Requestor shall write to the Trust to confirm that the Requestor has carried out the Trust's request and has fully complied with this agreement.

4. Information security undertaking

The Requestor hereby undertakes the following:

4.1 Where processing personal or sensitive information, the Requestor must comply in all respects with the provisions of the Data Protection Act 1998 and other relevant legislation (including any amendment or re-enactment thereof).

4.2 Shall fully indemnify the Trust against any claims arising at common law and/or

(a) under the Data Protection Act; and/or
(b) under other relevant legislation

as a result of a breach of the terms of this agreement.

4.3 Notify the Trust immediately of any notice or notification served on, or sent to, the Requestor Commissioner under the Data Protection Act. This particularly includes any de-registration, enforcement or transfer prohibition notice.

4.4 Notify the Trust immediately of any notice served on the Requestor regarding an individual in connection with any unauthorised disclosure of personal information.

4.5 Comply in all respects with the provisions of the Computer Misuse Act 1990 and Copyright Designs and Patents Act 1988 and of any other relevant legislation (including any amendments and/or re-enactment thereof).

4.6 Restrict access to personal information solely to responsible employees who need to have such access to it for the purpose of processing personal information and who have undertaken training in the use of personal information to a standard reasonably required by the Trust.

4.7 Not assign or sub-contract the whole or part of the processing of information to a third party without the prior written consent of the Trust.

4.8 Should the Trust agree to another party/sub-contractor (pursuant to clause 4.7), then that other party must first sign a copy of this Agreement as between it and the Trust, before carrying out any processing.

4.9 Allow the Trust on reasonable notice to inspect any premises where the processing of information takes place and for the Trust to inspect and copy any relevant documentation in order for the Trust to satisfy itself that the Requestor is complying with the provisions of this agreement.

4.10 Use best endeavours to immediately destroy or order the destruction of the information in the Requestor's control or possession, or at the Trust's request to return said information, (including any copies of the information on any media whatsoever), on completion of its use for the agreed purpose(s).

4.11 On destroying or returning the information the Requestor shall inform the Trust accordingly and the Requestor shall thereby warrant that the Requestor has acted accordingly.

5. Breach of confidentiality

The Requestor undertakes that:

5.1 Should a breach of this agreement occur by a member of the Requestor's staff, the Requestor shall immediately inform the Trust of the incident.

6. Jurisdiction and Applicable Law

6.1 The parties hereby accept the exclusive jurisdiction of the English courts and agree that the contract is to be governed and construed according to English law.

Instructions for execution of this Agreement:

Please indicate your acceptance of the above by signing this agreement in duplicate and returning both copies to the Trust. **Do not sign this Agreement unless you intend to be legally bound by its contents and obligations.**

The parties' authorised signatories must initial the left margin at clause 1, retrospective date, if this clause has been deleted.

For and on behalf of the Trust:

Authorised Signatory:
(Caldicott Guardian)

Name:

Title:

Date:

Authorised Signatory:
(Department Head)

Name:

Title:

Date

I/We agree to the terms contained in this agreement:

The Requestor's name:

Authorised Signatory:

Title:

Date:

Appendix 3

Pennine Care NHS
NHS Foundation Trust

SERVICE REQUEST: ICT SUPPORT – OFFICE MOVE

Please complete the following form, if you or your department are planning an office move which involves the repositioning of ICT equipment (This includes the moving of telephone headsets). This form should be fully completed and faxed back to 0161 716 3303 or emailed back to the ICT Servicedesk using **ictservicedesk.penninecare@nhs.net**

1. Co-ordinator of office move ***(Please provide Full name and contact details)***

Name:	
Job Title:	
Telephone:	
Location:	

2. Description of office move. ***(Please provide original location details and new location details)***

Estates Department Contacted – Yes/No Please provide Call ref: _____
Notes:

3. Scheduled date of office move
(Please note that the ICT Department require a minimum of 10 working days notice) DD/MM/YYYY

4.List of Equipment to be moved
(Please provide the Pennine Care security numbers and clearly state where the equipment is moving from and to)

PC's	Printers	Scanners	Faxes (include number)	Phones (include number)	Photocopier
TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL

5. Does the equipment need a new Network Point?* Yes / No *(If Yes you must order a Network point)*

Is there sufficient Electrical Sockets? Yes / No *(If No please contact Estates, Sockets cost approx. £125.00)*

**** Important H&S Notice only PC's/Printers within 3 metres of Network Point can be connected***

OFFICE USE ONLY

Asset Inventory Updated?	Yes ☐	No ☐	Service Request Reference:	
Additional Purchase Required?	Yes ☐	No ☐	If Yes, Order Ref:	
Active Directory Updated?	Yes ☐	No ☐	ICT Co-ordinator:	
Security Locks Refitted?	Yes ☐	No ☐	Date Move Completed:	DD/MM/YYYY

Appendix 4

Pennine Care NHS
NHS Foundation Trust

Department Name:						**Location:**			
NHS Number/ NI Number	**RT2 Number**	**Surname**	**First Name**	**DOB**	**DOD**	**Date Closed**	**Volume Number**	**Type of record**	**Date Destroyed**