POLICY FOR THE SAFEGUARDING, MOVEMENT & TRANSPORTATION OF PATIENT/CLIENT/STAFF/TRUST RECORDS, FILES AND OTHER MEDIA BETWEEN FACILITIES

Version 1_0

<p>| Name of Policy: | Policy for the Safeguarding, Movement &amp; Transportation of Patient/Client/Staff/Trust Records, Files and Other Media between facilities |
| Purpose of Policy: | To ensure that Trust staff follow a corporate approach towards the transportation of records between facilities and understand the importance of same |
| Directorate responsible for Policy | Performance and Reform |
| Name &amp; Title of Author: | Claire Graham Head of Corporate Records |
| Does this meet criteria of a Policy? | Yes |
| Staff side consultation? | Yes |
| Equality Screened by: | Claire Graham |
| Date Policy submitted to RM&amp;PC: | 14 January 2008 |
| Members of RM&amp;PC in Attendance: | Siobhan Hanna, Claire Graham, Roisin Toner, Kevin Gribben, Danny McKevitt, Anita Carroll, Carmel Harney, Mary Logan, Marie Austin, Fiona Wright |
| Policy Approved/Rejected/Amended | Approved with amendments |
| Communication Plan required? | Yes |
| Training Plan required? | Yes |
| Implementation Plan required? | Yes |
| Any other comments: | |
| Date presented to SMT | 6 February 2008 |
| Director Responsible | Performance and Reform |
| SMT Approved/Rejected/Amended | Approved |
| SMT Comments | |
| Date returned to Directorate Lead for implementation (Board Secretary) | |
| Date received by Office Manager (HQ) for database/Intranet | 11 February 2008 |
| Date for further review | 2 year default |</p>
<table>
<thead>
<tr>
<th><strong>POLICY DOCUMENT – VERSION CONTROL SHEET</strong></th>
</tr>
</thead>
</table>
| **Title** | Title: Policy for the Safeguarding, Movement & Transportation of Patient/Client/Staff/Trust Records, Files and Other Media between facilities  
Version: 1_0  
Reference number/document name: |
| **Supersedes** | Supersedes: C&B Legacy policy  
Description of Amendments(s)/Previous Policy or Version: Trust wide |
| **Originator** | Name of Author: Claire Graham  
Title: Head of Corporate Records |
| **RM/Policy Committee & SMT approval** | Referred for approval by:  
Date of Referral:  
RM/Policy Committee Approval (Date) 14 January 2008  
SMT approval (Date) 6 February 2008 |
| **Circulation** | Issue Date:  
Circulated By:  
Issued To: As per circulation List (details below) |
| **Review** | Review Date: January 2010  
Responsibility of (Name): Claire Graham  
Title: Head of Corporate Records |

**Circulation List:**

**All staff**
Policy for the Safeguarding, Movement & Transportation of Records and Files

Southern Health and Social Care Trust

POLICY FOR THE SAFEGUARDING, MOVEMENT & TRANSPORTATION OF PATIENT/CLIENT/STAFF/TRUST RECORDS, FILES AND OTHER MEDIA BETWEEN FACILITIES

1.0 INTRODUCTION

1.1 The aim of this policy is to ensure that staff safeguard all confidential information while travelling from one facility/location to another during the course of their working day.

1.2 This may include confidential information contained within work diaries, notebooks, case papers, patient/client notes, Trust documents, ‘lap top’ computers etc.

1.3 It is the responsibility of all staff to familiarise themselves with the contents of this policy.

2.0 GUIDING PRINCIPLE

2.1 The HPSS Guidance for the ‘Protection and Use of Patient and Client Information’ (June 1999), states that ‘everyone working for or with the HPSS who records, handles, stores or otherwise comes across information has a personal common law duty of confidence to patients and clients and to his or her employer. This applies equally to those, such as students or trainees, on temporary placements’.

2.2 Staff must notify their line managers immediately on suspicion of loss of any confidential information.

2.3 Managers must ensure staff are aware that disciplinary action may be taken when it is evident that a breach in confidentiality has occurred as a result of a member of staff’s neglect in ensuring the safeguarding of confidential information.
3.0 TRACKING / TRACING RECORDS

3.1 Managers must ensure that effective systems are in place for tracking the location of files containing confidential information. The type of system should be appropriate to the type of confidential information concerned (e.g. a card index system may be appropriate to a small department, while larger scale libraries may benefit from a computerised tracking system – e.g. PAS). Detailed guidance on tracking/tracing systems should be documented in departmental procedures and should take into account relevant professional standards where such exist. The following points should be incorporated into Departmental guidelines:

- A clear record of the files which have been removed from the designated storage area, and by whom, should be maintained;
- Files should be logged out to the borrower, who will be responsible for them whilst out of their designated storage;
- The tracking/tracing system should be updated by the borrower if the files are passed on, prior to being returned to the storage area;
- The minimum number of files required for the purpose should be removed;
- Files should be returned as soon as possible;
- A system for following up outstanding returns should be implemented;
- Responsibility for ensuring the availability of the files should be assigned to one individual within the Department.

4.0 MOVEMENT OUTSIDE THE WORK BASE

4.1 Movement of records off-site may be required for a variety of reasons, e.g.

- To facilitate care or treatment at a different Trust facility;
- To facilitate care or treatment at a different facility outside of the Trust;
- To facilitate patient/service user access;
- Recruitment, selection and other personnel functions;
- For domiciliary visits;
- To meet legal or statutory requirements;
- Delivery of drugs/specimens;
- For home working (where absolutely necessary)

(This list is not exhaustive)
5.0 RECORDS STORED IN THE PATIENT’S HOME

5.1 In some circumstances, records may be stored at the patient’s home e.g. maternity notes and Community Trust Home Care records. Confidentiality of the records stored in the client’s home is the responsibility of the client and they should be informed of their responsibility.

6.0 SAFEGUARDING OF INFORMATION TRANSPORTED BETWEEN FACILITIES/LOCATIONS

6.1 It is recommended that employees should avoid taking confidential information:

- Outside the work base wherever possible. However, it is accepted that there are certain circumstances where this will be necessary or unavoidable. Departmental procedures should detail the level of authorization required for the removal of files from Trust premises.

6.2 When files are removed from the Trust premises, it is vital that personal information is kept securely and the following guidelines should be followed to ensure it is adequately protected:-

- Keep the information in a secure container, for example a brief case or other suitable receptacle;
- Keep the information out of sight, for example in the boot of vehicles;
- Do not leave personal information unattended;
- If it is necessary to take personal information home, ensure that it is locked away and cannot be accessed by other family members or visitors;
- Make sure laptops and other software are kept securely, with documents containing personal information password protected.

Departmental procedures should detail any other specific requirements.

Related Policies/Manuals Include:-

1. The Protection and use of Patient and Client Information – Guidance for the HPSS (June 1999) [Link](http://hpssweb.n-i.nhs.uk/Data_protection/data_protect.htm)

2. Draft Code of Practice on Protecting the Confidentiality of Service User Information. Privacy Advisory Committee (NI) (June 2007) [Link](http://www.dhsspsni.gov.uk/confidentiality-consultation-cop.pdf)


