Northern Ireland Ambulance Service
Health and Social Care Trust

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

Title:	Policy for the Safeguarding, Movement and 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:	Finance and IT Directorate		
Name and Title of Author:	Miss Alison Vitty, Corporate Manager		
Staff Side Consultation	YES (via HR Joint Consultative Group 9 April 2009)		
Equality Screened:	YES		
Date Presented to:	ICT Committee	9 February 2009	
	Trust Board	7 May 2009	
	Comments	**APPROVED**	
Publication Date:	June 2009 Reissued – March 2016	Review:	June 2017
Version:	NIAS/TW/IG/4 (v3)		
(01) June 2009	No previous document to supersede. Specific Patient Report Form transportation guidance to be developed		
(02) June 2010	No amendments required. No change in legislative or good practice guidance		
(03) June 2013	No amendments required. No change in legislative or good practice guidance		

Circulation List:

This Policy was circulated to the following groups for consultation.

- Staffside
- Executive Directors and Senior Managers

Following approval, this policy document was circulated to the following staff and groups of staff.

- All Trust Staff
- Trust Internet Site/ Intranet Site

Policy for the Safeguarding, Movement and 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 whilst 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, human resource documents, patient report forms (further specific guidance to be developed), Trust documents, lap top computers etc.

1.3 It is the responsibility of all staff to familiarise themselves with the contents of this policy. This policy is complemented by the ICT Security policy which focuses on the safeguarding of information stored electronically.

2.0 Guiding Principle

2.1 The Department of Health, Social Services and Public Safety (DHSSPS) Code of Practice (January 2009) states that – "all users of our health and social care services have the expectation that any personal information they provide will be treated as confidential. However, the use and sharing of personal information forms an essential part of the provision of health and social care, benefitting individual users of the services and often necessary for the effective functioning of health and social services. Staff working within health and social services have an ethical and legal obligation to protect the information entrusted to them by users of the services".

2.2 Staff must notify their Line Managers immediately on suspicion of loss of any sensitive or confidential information. They in turn should advise the Corporate Manager.

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 neglect in ensuring the safeguarding of 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.

3.2 The type of system should be appropriate to the type of confidential information concerned eg a card index system may be appropriate in small areas or a computerised tracking/tracing system. Detailed guidance on tracking/tracing systems should be documented in Departmental procedures and take into account relevant professional standards where such exist. The following points should be incorporated into Departmental procedures:

- 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 be 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 files should be assigned to one individual within a 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;
- To facilitate patient/service user access;
- Recruitment, selection and other personnel functions;
- To meet legal or statutory requirements;
- For home working.

This is not an exhaustive list.

Staff must take all necessary steps to ensure that reasonable precautions are taken in order to minimise any breaches of confidentiality.

5.0 **Safeguarding Information Transported Between Facilities/Locations**

5.1 It is recommended that staff should avoid taking confidential information outside the workbase wherever possible. However it is accepted that there will be certain circumstances where this will be necessary or unavoidable. Departmental procedures should detail the level of authorisation required for the removal of files from Trust premises.

5.2 When files are removed from 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 briefcase or other suitable receptacle;
- Only the minimum amount of confidential information will be removed from secure Offices and only when it is essential for the member of staff to fulfil the requirements of his/her role;
- 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 it is locked away and cannot be accessed by other family members or visitors;
- Confidential information will not be left unattended and must never be left overnight in a car;
- Make sure laptops and other software are kept securely with documents containing personal information password protected.

6.0 Designated Accountability

The person accountable for overseeing the implementation of this policy and guidelines is the Corporate Manager.

7.0 Relevant Policies, Procedures and Guidance – Legislative Framework

Staff must comply with relevant legislation, professional standards and guidance and other DHSSPS publications as follows:

- Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order (Northern Ireland) 1925
- Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records (NI) Order 1993
- Human Rights Act 1998
- The Common Law Duty of Confidentiality
- Good Management, Good Records – DHSSPS, 2004
- Northern Ireland Records Management Standard (PRONI)
- Other NIAS Trust Policy and Procedures e.g IT Policies, Data Protection 1998 Policy, Records Management Policy

8.0 Equality and Human Rights Consideration

This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998. The Equality Commission for Northern Ireland Guidance states that the purpose of screening is to identify those policies which are likely to have a significant impact on equality of opportunity so that greatest resources can be devoted to those.

Following screening, no significant equality implications have been identified. The policy will therefore not be subject to an equality impact assessment.

9.0 Review of Policy

This policy will be reviewed in two years from the date of issue or as required with legislative or good practice recommendations.

Signed: _____

Liam McIvor (Mr)
CHIEF EXECUTIVE