Essex Partnership University
NHS Foundation Trust

TRANSFER/TRANSPORTATION OF RECORDS/INFORMATION/DATA PROCEDURE

POLICY REFERENCE NUMBER	CPG9f
VERSION NUMBER	2
REPLACES SEPT DOCUMENT	N/A
REPLACES NEP DOCUMENT	N/A
KEY CHANGES FROM PREVIOUS VERSION	Incorporated new General Data Protection Regulations Included the process for the recording of patient records transferring from North / South
AUTHOR	Records Manager
CONSULTATION	Information Governance Steering Committee Quality Committee Paris Project Board Mobius Project Board
IMPLEMENTATION DATE	April 2017
AMENDMENT DATE(S)	August 2018 (GDPR)
LAST REVIEW DATE	October 2018
NEXT REVIEW DATE	October 2021
APPROVAL BY IGSSC	September 2018
RATIFIED BY Quality Committee	October 2018
COPYRIGHT	

OPERATIONAL POLICY SUMMARY

These procedural guidelines will ensure that the transfer/transportation of Trust documentation is carried out in a secure, safe manner and that the confidentiality of sensitive information is maintained during the transfer of documents.

The Trust monitors the implementation of and compliance with this operational policy in the following ways;

Monitoring of compliance is undertaken via Local Managers, Records Management Team and the Information Governance Department.

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

TRANSFER/TRANSPORTATION OF RECORDS/INFORMATION/DATA PROCEDURE

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

TRANSFER/TRANSPORTATION OF RECORDS/INFORMATION/DATA PROCEDURE

Assurance Statement

These procedural guidelines will ensure that the transfer/transportation of Trust documentation is carried out in a secure, safe manner and that the confidentiality of sensitive information is maintained during the transfer of documents.

1.0 INTRODUCTION

1.1 Patients records and other Trust documentation contain person identifiable, confidential and/or sensitive information and care must be taken when transporting them within or outside of the Trust.

2.0 AIM OF THE PROCEDURE

2.1 The Trust has put in place an Information Governance and Security Policy and Procedures (CP/CPG50) and a Records Management Policy and Procedures (CP/CPG9) which set out the minimum policy standards for confidentiality, integrity, security and availability of information.

2.2 These procedural guidelines will enhance those policies and procedures and provide clear guidance on the transfer/transportation of Trust documentation with specific reference to manual and electronic records/information/data.

2.3 All clinical and non-clinical areas are required to observe and implement Data Protection Act 2018 principles when handling person identifiable information.

2.4 For the purpose of these procedures confidential information will include:

- person identifiable information
- sensitive information (about a person/s)
- other information that could be classified as ‘confidential’ such as that held by the Board or in work diaries

3.0 ROLES AND RESPONSIBILITIES

3.1 All staff are responsible for the safety and security of any health record/s that are created by them/tracked out to them.

3.2 All staff are responsible for the safety and security of any person identifiable, confidential and/or sensitive information that is to be transported.

3.3 All staff are responsible for adhering to the data protection principles and their duty of confidentiality.

3.4 Service, team, ward, senior managers are responsible for the security of records either health or corporate held within their working areas. When health records are tracked out of the main medical libraries/central stores the service, team, ward, senior manager will be responsible for ensuring the traceability of the health record/s in their clinical area/department.

3.5 Responsibility for the security of health records held within the medical libraries/central stores sits with the Trusts' Head of Electronic Systems & Records and IG and local records managers. Responsibility for records held in local community services sits with the local records managers, defined as the individual service/team manager.

3.6 All staff accessing record stores are responsible for ensuring the areas remain secure following legitimate access, e.g. locking doors, cabinets, drawers, once the record/s have been retrieved.

3.7 With the shift from paper records to electronic records all staff who access electronic records are responsible for ensuring their pc's are locked and secure when away from their desk.

4.0 GENERAL PRINICIPLES – INFORMATION GOVERNANCE AND DATA PROTECTION

4.1 Patients' health information and their interests must be protected through a number of measures:

- ensuring that all staff (including contractors, volunteers, temporary, locum, etc.) are fully aware of their responsibilities regarding confidentiality through information governance/record management training
- recording patient information accurately and consistently, maintaining high standards of record keeping
- keeping information private
- keeping information physically secure, ensuring that clinical/corporate records are stored safely (including the use of appropriate filing conventions)
- securing information whilst in transit (i.e. by car, on trains, walking, on buses etc.) This includes leaving packages etc. in cars and vehicles overnight or unattended.
- disclosing and using information with appropriate care

4.2 In practice this means that any person employed by the Trust is responsible for the health/corporate records they create or use, as established and defined by law:

4.3 All staff employed by the Trust (or who are contracted by the Trust) are obliged to observe a personal common law duty of confidence and work within the framework and principles set out in the Data Protection Act 2018 which places statutory restrictions on the use of personal information, including health information.

5.0 INFORMATION SECURITY

5.1 All incidences of breaches of confidentiality or near misses should be reported, via the Datix electronic incident reporting system where an investigation is carried out. Examples (not an exhaustive list) of such a breach are:

- correspondence or the health/corporate record/s has been wrongly addressed/delivered
- correspondence or the health/corporate record/s have not been securely delivered
- correspondence or the health/corporate record/s have been lost/stolen in transit
- correspondence or the health/corporate record/s has been found in an inappropriate place
- correspondence or the electronic health/corporate record/s have not been password protected when sent by email
- correspondence or the electronic health/corporate record/s have been sent to the wrong email recipient

5.2 Copies of Datix must be shared with the Trust Records Manager and the Information Governance Team by the Risk Team for investigation.

6.0 PROCEDURES

6.1 General Security Guidance

6.1.1 All staff should apply the following guidelines when involved in access, storage and/or transfer/transportation of health/corporate records:

- Keep doors/cabinets shut/locked when not in use and remove the key
- Store records appropriately so that they are not viewable by unauthorised persons
- Staff to wear ID badges and challenge the status of strangers
- Inform line/senior managers of anything suspicious (e.g. records not stored properly)
- Keep security systems/codes/procedures confidential – do not share with unauthorised personnel
- Be aware of the Trust information breach incident reporting processes
- Be aware of Trust procedures by which patients can request access to their records
- Always log out of any electronic system when task is completed
- Not reveal/share passwords/log-in codes to others
- Change passwords/log-in codes regularly avoiding the use of obvious words such as familiar names, holiday destinations, etc.
- Use of screen savers and obscure angles of screens to prevent casual viewing
- When transporting in vehicles records should be kept in a sealed bag or carrier and be out of sight in the vehicle, in the boot (i.e. not stored in the foot hold of the passenger seat or behind the

seats, in the back of the car, on the floor) if no boot is available (this will be the case in extreme cases and the service manager must be notified to ensure a risk assessment can be undertaken) and removed immediately upon destination
- Vehicles must never be left unlocked when not in attendance, even for a short period of time
- All courier drivers must ensure all items are removed from their vehicle and stored in the designated cupboard / post room

    - Severalls Hospital – in the post room lockable cabinet with the building alarm set when unoccupied
    - The Rowans, Room no. 3:33 – grey lockable cabinets within room restricted access
    - Derwent Centre post room with restricted access

6.2 Prior to Transfer/Transportation of Records

6.2.1 Prior to the transfer/transportation of any records to *external* sources the record must be reviewed by the responsible medical/clinical/professional to ensure the integrity of the record, this must follow the Trusts Access to Records procedure.

6.3 Procedure for the Transfer/Transportation of Manual Records

6.3.1. Via Central libraries

6.3.1.1 Manual records being dispatched from any of the Trust's Medical Records libraries must be:

- Formally booked out of their filing system (electronic tracker or tracer cards)
- Where appropriate, tracked using the Trust information system
- A detailed list of the records included within the transfer must accompany the records and this must be signed for by both the sender and receiver.
- The Courier service needs to sign upon collection and delivery using their appropriate paperwork.
- Transferred between clinical areas, clearly labelled, using the Trust approved methods, for example:
    - Tagged medical records bags
    - Lockable medical records crates
    - Covered/lockable medical records trolleys
- Once delivered to its destination the record/s must be stored securely (locked away when not in use) within the clinic, ward or office environment, inaccessible to non-authorised persons and stored in a manner that the record can easily be found if urgently required
- Returned to the appropriate central record store as soon as possible after use

6.3.2 By Staff

6.3.2.1 Manual records being transported with staff must be:

- Formally booked out of their filing system (using tracer cards)
- Where available, tracked using the Trust information system
- Sealed in a Trust approved carrier, e.g. tagged medical records bag, lockable briefcase
- Stored out of sight if being transported in a vehicle in the boot of the car and removed immediately upon destination – where one or more records are being transported (e.g. for the purpose of home visits with clients) all records must be kept with the staff member at each individual home visit and never left unattended in the vehicle
- Staff should not normally take health records home (either hard copy or electronically) however this cannot always be avoided and the following procedures should be adhered to safeguard information effectively:

    - Ensure records are tracked out and traceable
    - Ensuring records are not left in vehicles overnight
    - Ensuring stored in locked cabinets/drawers /trolley cases/ sealed bags
    - Ensuring return to the record store as soon as possible
    - Obtain the permission of your manager

6.4 Procedure for the Transfer/Transportation of Electronic Records

6.4.1 The Trust has the technology to burn electronic records onto encrypted CDs and other portable devices (as approved) for the transportation/transfer of records. All staff must ensure that this process is adhered to for the transfer of electronic records and that USB devices, unencrypted discs, etc. are not used. Requests for this type of encryption should be directed to the Trust Records Manager.

6.5 Transfer/Transportation of Health Records Out of Hours

6.5.1 Between 8am – 5pm, Monday – Friday medical records staff are available to assist with the tracking, transfer and transportation of health records.

6.5.2 If a health record/s is required out of hours, the requestor, via the Contact Centre can contact the on-call officer who will have the authority to arrange for the record/s to be released.

6.5.3 This guidance procedure for the transfer/transportation of health records applies to both core working hours and ‘out of hours’ requests.

6.6 Transfer/Transportation of Records Outside of the Trust

6.6.1 The Trust Access to Records Department will receive requests for records outside of the organisation and Trust policy is not to send original copies except in defined circumstances, e.g. when the case notes are accompanying the patient being transferred out of hours or for records requested by a Court.

6.6.2 Where these records are being sent outside of the organisation, as paper records, they must be securely packaged in polythene envelopes (for order details of this product contact the Records Manager), sealed and labelled (Addressee Only, Private & Confidential) in line with Safe Haven procedures. The records should be posted via the external mail using Recorded/Special Delivery services. On the back a label is to be added stating if undelivered please return to PO Box 2213 plus the courier code (for the South locality) and the building name (for the North Locality) plus staff initials Where there are several packages/particularly large packages the sender may need to consider the use of authorised courier services (advise on authorised courier services can be obtained from the Trusts Records Manager). Wherever possible paper records should be scanned and sent electronically using encryption, password protection and email facility to mark as Private & Confidential.

6.6.3 Where the record/s are held in electronic format (e.g. CD) the portable device must be encrypted in line with Trust policy. Requestors will be asked to call the Access to Records department for the password

6.6.4 Where courier services are used it is essential to confirm that the courier service has tracking systems in place, including recording of collection/delivery and traceability of the package.

7.0 Process for North / South patients records recording / transfer

7.1 At times there will be a need to transfer North or South patients to each location. For the purpose of this process we will assume we are transferring a patient to North from South
The electronic patient record system of the receipting ward will need to be completed (Paris UDF's – North, Mobius eForms – South) and saved as per normal practice.

- Electronic forms or templates to be completed
- Paper forms should be kept to a minimum
- Paper forms should be scanned on as per normal practice
- Separate paper files should not be collated

If the patient is subsequently transferred back to their originating area, a subset of the documents should be transferred with the patient via Health Information Exchange (HIE) these include:-

- Alerts
- Demographic details
- Initial and risk assessment
- Care plan
- Consent
- Medications
- Legal / detention paperwork if applicable
- Any other key documents as required at the time
- *This list is not exhaustive*

7.2 All clinical staff can have access to the Health Information Exchange (HIE) where key documents have been uploaded in readiness to be viewed.

If additional clinical documentation is required, this can be facilitated via the records team during office hours or out of hours by direct contact with the previous ward. Information can be emailed or faxed ensuring safe haven methodology is used

7.3 Any paper documentation transferred, will be scanned (by ward administrators or other admin / Medical Secretariat) to the receiving electronic records system in the appropriate sections to aid future reference.

END