Standard Operating Procedure Template

Title of Standard Operation Procedure:	Transportation/Disclosure of Identifiable Information
Reference Number:	**Version No: 2.1**
Issue Date: Oct 2016	**Review Date: Oct 2019**
Purpose and Background	To ensure that all staff, both Acute-based and Community-based, are aware of the requirements when transporting identifiable information.
Scope (i.e. organisational responsibility) Vital functions affected by this procedure:	All staff

Monitoring Compliance						
Requirement to be monitored. Must include all requirements within NHS LA Standards	Process to be used for monitoring e.g. audit	Responsible individual/ committee for carrying out monitoring	Frequency of monitoring	Responsible individual/ committee for reviewing the results	Responsible individual/ committee for developing action plan	Responsible individual / committee for monitoring action plan

Escalations (if you require any further clarification regarding this procedure please contact):	Information Governance Officer

	Committees / Group	Date
Consultation:	Health Records Management Sub-Group	**23/08/16 and 25/10/16**
Approval Committee	Information Governance & Records Management Group	
Ratified by Committee	Information Governance & Records Management Group	
Received for information:	Trust Internet	

Contents

1. Introduction 4

2. Guidance 4

3. Monitoring 8

OPERATING PROCEDURE

1. Introduction

Principle 7 of The Data Protection Act 1998 – Information must be secure – includes the requirement that '*appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'*. The Trust's requirement to transport information both to and from the Acute site as well as in the Community is covered by this principle.

The NHS document Information Security: NHS Code of Practice (based on the internal standard in Information Security – ISO 27001) requires that there are adequate controls to secure any 'media in transit'. This Standard Operating Procedure has been produced to provide guidance to all staff and to ensure a consistent approach to the transportation of information across the Trust and all staff are required to review its contents and to follow the recommendations to minimise the risk, specifically:

- When transferring paper-based records internally across the Trust footprint using the internal mail service, the Trust's contractor (ERS Medical) must be used ensuring that appropriate packaging is used and that an accurate and complete delivery address is clearly displayed.

- When transferring paper-based records across the Trust footprint by hand (for example when visiting patients at home), secure packaging must be used e.g. Trust blue bags; briefcase; rigid lidded container.

- Information transferred on a memory stick **MUST** be a copy via an encrypted stick, with the original stored on the Trust's secured network drives.

- Transferring information using e-mail **MUST** be via the 'NHS.net'. Sending e-mails from a Trust 'nhs.net' e-mail account to another 'nhs.net' e-mail account is secure' 'nhs.net' to 'nhs.uk' is NOT secure and identifiable information must not be transferred this way. A list of secure domains is attached as Appendix 1, for those staff needing to transfer to other public authorities.

2. Guidance

All staff are responsible, within their terms and conditions of employment as well as the Trust's Policies and Procedures, for safeguarding the security and confidentiality of identifiable information. This includes adherence to the Data Protection Act 1998 which states that information must only be accessed on a strict need to know basis. This requirement applies whether information is accessed on Trust sites or in the community.

For the purposes of this operating procedure, 'information' can take any form – paper records; correspondence; digital images; electronic records; video tape; audio tape, for example and the contents apply to anything which has the potential to identify any individual either by means of a name, patient number, address, NHS number.

Information required off-site, for example, at multi-disciplinary meetings or when visiting patients at home is particularly vulnerable to inappropriate access, loss or misuse. This information must be transported securely using the guidance contained in this Operating Procedure and must be returned to the office as soon as possible.

2.1 Transporting Information via Internal Mail

- The Trust's approved transport contractor is ERS Medical. All staff should familiarise themselves with local procedures in terms of collection/ delivery times.
- All patient case notes leaving the trust should be contained within either:
  - Case notes for clinics being held out in Community Locations should be in robust lidded containers specifically designated for transportation.
  - Case notes being returned from Community clinic locations should be returned to the trust in the same container clearly labelled for the receiver.
  - Patient information and ad hoc case notes should be delivered to Community Locations via the Health Records Library 'Blue Box' system.
- Delivery address information to be confirmed and must be clearly displayed on the packaging with previous addressee information removed (when using recycled envelopes), to include the name/job title of the recipient together with base information.
- If sensitive information is being sent via the internal mail system, it must be clearly marked 'Private & Confidential'.
- With regard to Admin. staff opening mail, local procedures should be adopted according to the wishes of the senior clinician however bearing in mind that all staff are required to adhere to the Trust's Policies and Procedures with regard to the need for confidentiality, the following guidance is provided to assist:-
  - 'Private & Confidential' to be used for sensitive business information which, depending on local procedure, is appropriate for admin staff to open.
  - 'Personal'; 'To Be Opened By Addressee Only' tends to refer to information that is specific to the addressee and may not be business-based – these should be left for the addressee to open.
- Any instances where confidential/sensitive PID information fails to reach its destination should be reported according to the Policy for the

Management and Investigation of Incidents, Complaints and Claims Including the Analysis of Data:-

http://www.eastcheshire.nhs.uk/About-The-Trust/policies/I/Incidents%20Complaints%20Claims%20Management%20ECT2103.pdf

2.2 Transport Information via External Mail (please refer also to Policy for Release of Hospital Case Notes to Social Services and other Healthcare Professionals)

- External mail to be handled according to the requirements contained within (2.1) above, including the requirement to report any instances where information fails to reach its destination.

- Every effort must be made to ensure that contact information on record is accurate and up to date, to reduce the risk of information being inappropriately addressed. Best practice suggests that contact information is confirmed by admin/reception staff at each appointment.

- Individual teams must have a process in place to update the Master Patient Index when contact information is found to be out of date.

2.3 Transport Information via Taxi (please refer also to Policy for Release of Hospital Case Notes to Social Services and other Healthcare Professionals)

On occasions, information is required to be transported urgently, for example to neighbouring NHS Trusts for emergency procedures. On these occasions it is appropriate to transport via taxi following these guidelines:-

- Approval from line management is required **before** proceeding.
- Taxi to be booked via the Switchboard.
- Information to be secured in tamper-proof envelopes which can be located in the switchboard office, securely sealed with the intended recipient **clearly marked** with the exact location, marked ‘Private & Confidential’ with a return address included on the envelope.

2.4 Transporting Records Off Site By Hand

- For the purposes of this section, the requirements contained within (2.4) apply to the use of Paper Diaries for community staff.
- When visiting patients at home, ensure that any records carried at the same time cannot be seen by any member of the household (including family, friends and neighbours, children or parents)

- Staff should advise patients who are in possession of patient-held records that the information is personal to the patient and should not be viewed by other members of the household without the patient's consent.

- When transporting information by car, the requirements regarding the packaging are as noted above i.e. secure/lockable/tamper-proof packaging; briefcase

- Information must be transported in the locked boot of a car (i.e. not left on view).

- Information must not be left unattended. Where possible all information is taken into the patient's home. If this is not possible, information MUST BE stored out of sight in the car's boot.

- Information MUST NEVER BE LEFT IN THE CAR OVERNIGHT

- Information must not be recorded on a home PC. If staff are required to undertake work at home, an encrypted memory stick must be used and the information transferred to the Trust's secure network as soon as possible.

2.5 Removable Equipment & Electronic Media

- Removable media is defined as being any device that can store information when not attached to a static device (PC). This will include (but is not limited to):

  - Laptops
  - Smartphones (IPhone/Blackberry etc.)
  - CD
  - Audio Tapes/Video Tapes
  - USB Memory Sticks/Cards
  - Portable Hard-Drives
  - SIM Cards

- East Cheshire Trust requires that all removable media is encrypted and the use of non-encrypted devices for the transportation of PID information is not permitted according to the Trust's Policies and Procedures. All staff using removable media are responsible for the secure use of that media.

- Where information is required to be transferred electronically, the preferred method is via the Trust's secure e-mail network – NHS.net. Details of alternative Secure Networks in use by Partner Organisations is included at Appendix 1. Information MUST NOT be sent by e-mail using a domain that is NOT listed in Appendix 1.

- When sending a removable device via the mail system (either internally or externally) the information contained on the device MUST be password protected and the password is to be sent separately from the device.

- Any loss of a removable device must be reported according to the Trust's Policy for the Management and Investigation of Incidents, Complaints and Claims Including the Analysis of Data:-

http://www.eastcheshire.nhs.uk/About-The-Trust/policies/I/Incidents%20Complaints%20Claims%20Management%20ECT2103.pdf

2.6 Faxing

- Information transferred via Fax must be sent according to the Trust's Safe Haven procedure.

- In brief, the following must be observed:

  - All receiving fax machines must be designated as a Safe Haven fax

  - Only the minimum information to be sent

  - When faxing to a new recipient – a test fax must be sent with the recipient confirming receipt, before any PID is transmitted.

- All Fax ribbons must be disposed of in the confidential waste and must not be placed in the general waste.

2.7 Transferring/Disclosing Information over the Telephone

- All staff must be aware of the risks involved when disclosing information over the telephone. Information about a patient must never be disclosed without first verifying the caller's identity and eligibility to receive the information and the use of a password system/security question is recommended, such details to be recorded on the patient's record on admission.

- Where a password system has not been organised in advance, staff must assure themselves by means of asking the caller to provide identifiable information relating to the patient and only the minimum of information to be disclosed. Under no circumstances is the patient's medical condition to be disclosed unless the patient has given explicit consent for this information to be divulged - in which case the identity of the person receiving the information must be verified and matched against consent which has been previously obtained and recorded in the patient's record.

- As stated above, the use of a password system/security question is recommended in dealing with relatives' enquiries received by phone. This information to be recorded in the patient's record on admission and all staff to be aware.

- If a caller requesting personal information claims to be from an external agency such as the Police they should be phoned back via the switchboard of the organisation they are calling from.

- When contacting patients by telephone and/or leaving a message, staff must be conscious of the need for confidentiality. It is appropriate to introduce yourself 'Nurse Jane Doe from East Cheshire NHS Trust'. Under no circumstances must any sensitive/confidential information be disclosed in a telephone conversation until you are satisfied that you are talking to the patient. Sensitive/confidential information must never be left in an answerphone message, instead request the patient to call back or identify a convenient time for you to call the patient.

3 Monitoring

The contents of the procedure will be subject to review via spot check audits, carried out on a regular basis according to a random rolling programme.

APPENDIX 1

The following domains (listed below) are all **Secure**. E-mails sent from an NHS.net account to any of these domains are secure and can contain Person Identifiable Information. Currently, these are the only secure domains to be used – the list will be updated as and when security is assured on additional e-mail domains:

- **NHS (*.nhs.net)**
- **GSi (*.gsi.gov.uk)**
- **CJX (*.police.uk or .pnn.police.uk)**
- **GSE (*.gse.gov.uk)**
- **GSX (*.gsx.gov.uk)**
- **GCSX (*.gcsx.gov.uk)**
- **SCN (*scn.gov.uk)**
- **CJSM (*cjsm.net)**
- **MoD (*.mod.uk)**