Transportation of Health Records or Confidential Information Within and Outside Charity Premises

Title:	Transportation of health Records or Confidential information Within and outside Charity premises
Procedural document Type:	Policy
Reference:	CL 039 V3
Version:	3 Three
Approved by:	Clinical Governance
Date Approved:	13.3.19
Ratified by:	Clinical Governance
Date Ratified:	13.3.19
Name or originator/author:	Richard Ward – Information Governance
Name of responsible team:	Clinical
Review Frequency:	Three years or when changes in legislation occur
Review Date:	March 2022
Target Audience:	All Staff

Contents

Please Note the Intention of this Document

Please see Introduction

Review and Amendment Log

Version No	Type of	Date	Description of change
Two	initial	June 2017	Initial Document
Three	Updated	Feb 2019	Updated for GDPR

1. Introduction

Although these Guidelines refer specifically to Health Records the same principles apply to all personal and confidential information including staff, volunteer, donor or supporter records as well as commercially confidential information.

Patients' Health Records contain personal and sensitive information and are highly confidential documents. Care must be taken when transporting them within or outside the Charities premises. This guidance applies to transfers between Hospices and to and from Community Hubs or other places where Charity records may be required or created.

2. Purpose of the Guidelines

These Guidelines cover the overlapping areas of data protection compliance, information security, data quality and confidentiality.

Their purpose is to provide guidance for the security and transportation of confidential information with specific reference to manual and electronic health records.

All clinical and non-clinical areas should observe and implement the GDPR and Data Protection Act 2018 principles when handling information about identifiable individuals (Appendix 1).

For the purposes of these Guidelines, confidential information will include personally identifiable information. However the same procedures can apply to 'sensitive' information and other information that could be classified as 'confidential' which is also held by the Charity such as information held in work diaries.

2.1. Information Governance and Data Protection – General Principles

Patient's health information and their interests must be protected through a number of measures:

1. Procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality
2. Recording patient information accurately and consistently
3. Keeping information private
4. Keeping information physically secure

5. Disclosing and using information with appropriate care

In practice, individuals employed by the Charity are responsible for any health records they create or use. This responsibility is established at, and defined by, law.

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

All members of the healthcare team have a responsibility to:

- Maintain high standards of record keeping
- Ensure that records are stored safely and securely (including use of an appropriate filing convention)

3. Information Security

The following occurrences concerning a health record, x-ray or personal patient information should be subject to the completion of an incident form (see Appendix 2) and an investigation carried out:

1. Where correspondence or the health record has been wrongly addressed/delivered
2. Where correspondence or the health record has not been securely delivered
3. Where correspondence or the health record has been lost in transit
4. Where correspondence or the health record has been found in inappropriate location

4. Transportation of Health Records within the Hospices

The following procedure, shown as a checklist, applies to all staff involved in the transportation of health records or who have access to health records within the hospices.

All staff must observe the rules shown below to ensure the security of health records:

a. Shut/lock doors and cabinets as required
b. Store records appropriately so that they are not viewable by unauthorised persons.
c. Wear ID badges
d. Challenge the status of strangers – if considered safe to do so
e. Inform their manager or senior manager (as appropriate) if they witness anything suspicious or worrying (e.g. records not properly stored)
f. Not inform unauthorised personnel how security systems/procedures within their department operate.
g. Not breach confidentiality and security themselves
h. Be aware of the procedure by which incidents relating to breaches of patient confidentiality and information security are reported (see Appendix 2)
i. Be aware of the procedure by which patients can request access to their health record.

4.1. Manual records must be:

a. Formally booked out of their filing system
b. Tracked appropriately
c. Returned to its filing location as soon as possible after use
d. Stored securely within the clinic, ward or office environment, arranged so that the record can be found easily if urgently needed.
e. Stored closed when not in use so that contents are not seen accidentally
f. Inaccessible by members of the public and not left even for short periods where they might be overlooked by unauthorised persons.
g. Held in secure storage with clear labelling.
h. Transferred between clinical areas either in a sealed records transfer pouch (the zipped blue pouches) or in a medical records trolley.

4.2. With electronic records staff <u>should</u>:

1. Always log out of any computer system or application when work on it is finished.
2. Not leave a PC unattended and logged in
3. Not share passwords with other staff. If other staff need to have access, the appropriate access should be organised for them via the IT team
4. Not reveal passwords to others
5. Change passwords at regular intervals to prevent anyone else using them
6. Avoid obvious passwords like names, addresses.

7. Always clear the screen of previous patient information before seeing another.
8. Use a password protected screen saver and move monitors to prevent casual viewing of patient information by others.

5. Transportation of Health Records, Out of Hours

Between 9am and 4:30pm on weekdays, Medical Records personnel are available to assist with the tracking and transportation of health records between hospices/departments if required. If a set of case notes is needed out of hours, then the case notes will be retrieved by on duty clinical staff (who are trained to use the tracking system) and are also authorised to track and transport case notes out of hours – the procedural rules apply to both core working hours and 'out of hours'. In urgent cases this tracking may need to be after the event.

6. Transportation of Health Records between Sites and Locations used by the Charity e.g. Community Hubs

Where patient identifiable information or patient records are created or taken off site, the following guidance must be observed.

Staff should not leave portable computers, medical notes or mobile data devices (e.g. Dictaphones, PDAs, digital cameras) that are used to store patient records/patient identifiable information in unattended cars or in easily accessible areas. Ideally store all files and portable equipment under lock and key, when not actually being used.

Staff should not normally take health records home (either in hard copy or electronically) and where this cannot be avoided, procedures should be place to safeguard that information effectively.

This includes the following actions:

- Undertaking a risk assessment regarding the storage and safety of the records
- Putting in place systems to ensure the records can be accessed in an emergency if needed
- Ensuring that the records are tracked out and traceable
- Ensuring that permission has been given by the Caldicott Guardian for health records to be stored away from a recognised base for health records storage.

Any records taken offsite must be properly secured preferably within a container in the boot of the car; they should never be on open view on a seat. Care needs to be taken with hatchback cars to ensure the hatch cover is in place to ensure the contents in the hatch are not visible.

Staff should not use their own equipment to store any patient identifiable data. In exceptional circumstances staff may use their own equipment to store patient identifiable data, but only with the express written permission of the Caldicott Guardian who will be satisfied of the need to do so and that appropriate safeguards are in place.

Any such permission should be specific in terms of what information may be stored, for how long and how it will be protected. Failure to comply with these conditions may result in disciplinary proceedings.

Any personal devices used must be registered with the IG Officer, via the IT Department. Portable computing devices (e.g. data sticks) will be issued with encryption software for use by staff with the requirement to transfer data by this means.

7. Physical Controls

Health records should be transported in either sealed boxes or sealed pouches when being transported between hospice sites and locations.

Health records should be hand delivered for internal transfer (personally to the recipient and not left in an unattended office) and not put into the internal mail. All records should be tracked from the current location to the new location to ensure traceability at all times.

8. Transportation of Original or Copy Health Records to Hospitals or Authorised Agencies outside the Internal Mail Delivery Service

The Charity policy is not to send original health records outside the Charity except in strictly defined circumstances. The exceptional circumstances include case notes accompanying patients who are transferred to another hospital out of hours or records requested by the Court.

Where original or copy case notes are sent via external mail, high grade envelopes or two envelopes must be used to provide adequate protection for the contents, and they must be sent via special delivery or registered mail.

If health records held in electronic format are being sent by post, then the data must be encrypted (e.g. sending data such as a diagnostic tests or images etc. on a CD/memory stick via special delivery or courier). Heads of department responsible for sending documents in electronic format, should contact ICT/Information Governance to discuss how to put in place processes for encryption and decryption.

The NHS courier service may be used but if an external Courier service is being used, then it is essential to confirm that the Courier service has tracking systems in place, including recorded delivery and traceability of packages.

In these circumstances, and for other personal information sent by external mail the addressing must be accurate, and the senders name and address must be given on the reverse of the envelope.

9. Lifting and Handling of Health Records

Health records should be handled safely and in accordance with the Charities manual handling policy.

In terms of general principles, to avoid injury health records should be transported by trolley between locations. Health records should be kept to a maximum thickness of 2 inches and additional volumes created for 'fat files'. All volumes should be tracked and traceable as per the guidelines set out in this policy.

10. Staff Transportation of Health Records

Health records should be transported in sealed envelopes or pouches (whether this is personal delivery by staff or NHS courier). If health records are being transported in larger numbers, then they should be sealed in boxes or safely moved around using a medical records trolleys.

Health records which are being moved by Charity vehicle (e.g. car or van) must be stored in a sealed container (either envelope, pouch or box). Health records should never be left unattended in a vehicle or visible to the public. Also see the previous sections for information about physical security of health records

11. Roles and Responsibilities

All staff are responsible for ensuring the safety and security of health records, which are tracked out to them. Maintenance of data protection principles and confidentiality are requirements set out at a contractual level for all staff employed by the Charity (including independent contractors).

In terms of general principles, service managers also need to be aware that they have specific responsibilities for the security of health records held in their areas. When health records are tracked out from the main filing system, the service manager is responsible for ensuring the traceability of the health records held in their clinical area or department.

12. Patient Requests to Access Medical Records

Requests from patients to access their health record should be addressed to the Director of Patient Services in the first instance. There is a specific procedure in place, which must be followed to facilitate patient access to their health record.

Appendix 1 - Data protection principles

A summary of the 8 data protection principles:

1. Personal information must be fairly and lawfully obtained
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept for longer than is necessary
6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection

Appendix 2 - Information incident reporting process

In the event of a suspected information security or confidentiality breach occurring the following process should be followed:

All incidents, suspected incidents and near misses should be reported as soon as practically possible (normally within 24 hrs)

- The person discovering an actual or suspected information breach or incident should report it to their line manager (this includes near misses), and
- The line manager should ensure action is taken to contain the incident/prevent a recurrence.
- The incident should be reported to the area's Executive management, and
- an Information Incident Report form (see next page) should be completed and sent to the Information Governance (IG) Officer (rward@cornwallhospice.c.uk).
- IG will carry out an assessment and determine, in conjunction with management, what investigation is needed,
- who should carry it out and
- who should receive the report.
- The IG Officer will ensure the Caldicott Guardian is made aware of the incident.
- All reported IG incidents are logged onto the NHS Incident Reporting system, and
- reported through the IG Forum.

The Information Incident reporting form is located in the Information Governance/Public IG Library folder on the CHC Intranet (Office 365), or may be obtained by contacting the IG Officer by email or on 01726 66868 Option 7.

INFORMATION INCIDENT REPORTING FORM

Location of incident:

Date of incident:

Which of the following best describes the incident *(please tick one):*

Lost digital equipment eg laptop computer	
Theft of digital equipment eg laptop computer	
Lost information (paper/digital eg USB stick)	
Theft of information (paper/digital eg USB stick)	
Information Breach - Post	
Information Breach - EMail	
Information Breach - Fax	
Other Breach of Information Security	

Other (please specify):

Details of the incident (please focus on facts rather than opinions):

Immediate action taken (if any):

Further planned/required actions (if any):

Form completed by: _____ Date: _____

Please return to: **Richard Ward** (information Governance Officer)
rward@cornwallhospice.co.uk
Tel: 01726 66868 Option 7

IG Use:
Action: Ref No: