Cornwall Hospice Care
Caring for our community
Mount Edgcumbe Hospice St. Julia's Hospice
Registered Charity No. 1113140

Health Records Policy

Title:	Health Records Policy
Procedural document Type:	Policy
Reference:	CL - 035
Version:	Version 1
Approved by:	Clinical Governance
Date Approved:	13.3.19
Ratified by:	Clinical Governance
Date Ratified:	13.3.19
Name or originator/author:	Richard Ward
Name of responsible team:	Information Governance
Review Frequency:	3 years or when changes in legislation occur
Review Date:	January 2022
Target Audience:	Clinical staff and clinical administration staff

Contents

Please Note the Intention of this Document

This document describes how Cornwall Hospice Care (CHC) is committed to the principle of maintaining accurate, comprehensive, clear and complete records of the condition, care and treatment provided for all patients and carers. The records will be kept for the appropriate periods as laid down in legal and national requirements, used appropriately and safeguarded against damage, loss or improper use.

Review and amendment Log

Version No.	Type of Change	Date	Description of Change
Version 1	New	Feb 2019	New document

Introduction

1. Cornwall Hospice Care (CHC) is committed to the principle of maintaining accurate, comprehensive, clear and complete records of the condition, care and treatment provided for all patients and carers. The records will be kept for the appropriate periods as laid down in legal and national requirements, used appropriately and safeguarded against damage, loss or improper use.
2. CHC currently employs paper based patient records although these may be analysed using electronic systems to provide management information.
3. CHC is aware of the increasing requirement to use electronic information systems and to share patient information between service providers. These changes facilitate more effective, integrated treatment and care but increase risks with regard to breach of confidentiality and inappropriate use. CHC is committed to developing systems, understanding and skills that ensure that these requirements are met within an appropriate and effective information governance framework.
4. CHC will ensure good governance of information generated internally. CHC will also take due care to protect information received from partner organisations or individuals and to provide assurance of the security of such information. This will include, where appropriate, the adoption of relevant information governance standards and, where required, Information Sharing Agreements.
5. No person will be provided with access to health records without first:
    - being provided with, and reading, a copy of this policy;
    - receiving training in the use of CHC records system and confidentiality requirements.
    - completing mandatory Information Governance training
6. This document sets out the methods by which records are created and the requirements for staff to complete and use records appropriately. In combination with the 'Organisational Records and Information Management Policy' and associated procedures, it covers requirements for the creation, access, management, handling, transportation, storage, destruction of records, what to do when an error occurs and the monitoring of these processes.
7. These requirements apply to all patient and service user records held across the organisation.

Duties

8. Broad managerial and professional responsibilities in respect of this policy are set out in the Governance Policy.

9. In respect of this policy, these additional accountabilities and authorities are established:
    - The Medical Director: as Caldicott Guardian, carries responsibility for providing advice and guidance on complex service user confidentiality issues.
    - The Medical Director and Director of Patient Services provides professional leadership in respect of the quality of service user records and records audit.
    - The Director of Education and Governance is the Information Asset Owner of Patient services data.
    - The IT Manager is the technical lead responsible for ensuring that electronic information systems are secure and available to meet service requirements.
    - The Quality Assurance Officer is responsible for the monitoring of the quality of patient data via audits.

Procedure for Health Records Management, Storage and Destruction

The Charity committed to the principle of maintaining accurate, comprehensive, clear and complete records of the condition, care and treatment provided for all patients. The records will be kept for the appropriate periods as laid down in CHC Records Retention Schedule, which takes into account legal and national requirement, and safeguarded against damage, loss or improper usage.

Aim and Scope of Procedure

To set out the steps by which health records are created, the requirements of clinical staff to complete the records appropriately and the requirements for the management, handling, storage and destruction of health records.

Staff Responsibilities

Director of Patient Services

Responsible for ensuring that health records are maintained for all patients and adhered to.

Director of Education and Governance

Responsible for ensuring that the content of the policy and procedure is in line with statutory a requirements and professional guidance. Ensures that clinical staff and other staff, as appropriate, are aware of the policy and procedure and how to apply it. Ensures that patients are aware through the provision of suitable information materials.

Clinical staff

Responsible for compliance with the policy and procedure

Access to Health Records by Patients and Authorised Representatives

All patients have the right to see and receive a copy of information we hold about them in their Health Record. This is known as the right of subject access.

The right to subject access is contained two acts of parliament:

- General Data Protection Regulations
- The Access to Health Records Act 1990 -covering access to the records of deceased patients.

If you believe you have received a subject access request you should pass the details to the Director or Education and Governance who will make arrangements for it to be dealt with.

Subject access requests will be processed within 28 days and at no cost to the requestor.

Method:

Creation of health records

All patient health records are kept in the standard hospice health record folder (Integrated notes folder) which holds all papers securely, allows insertions to be made and clearly indicates the location of each part of the health record.

Each patients' NHS number is recorded on all documentation relating to that patient.

Completion of the record

All members of the multi-professional care team are responsible for keeping records of their interventions with patients and observation records, as appropriate in line with their respective professional body guidance (see Appendices C,D,E).

The purpose of the health record is to:

- provide accurate, current, comprehensive and concise information concerning the condition and care of the patient and associated observations
- provide a baseline observation record against which improvement or deterioration may be judged
- provide a record of any problems that arise and the action taken in response to them
- provide evidence of care required, interventions carried out and patient responses
- include a record of any factors (physical, psychological or social) that appear to affect the patient
- record the chronology of events and the reasons for any decisions made.

Entries in the patient records must be:

- written legibly in ink *(black ink is recommended)*
- clear and unambiguous
- dated
- timed (this may not always be the case for outpatient/community notes)
- signed by the person making the entry with the person's name and designation next to the signature
- It is not good practice to use abbreviations in health records and these should be avoided as much as possible.
- Alterations are made by scoring out with a single line, which should be signed and dated against so that the original entry can still be read alongside the correction. Liquid paper, adhesive paper or Tippex must not be used to delete on error.
- If an entry into the health records are in error (i.e. Wrong patients notes), the entry should be scored out with a single line, signed, dated and highlighted as written in error.
- All entries made by students or non-qualified staff must be countersigned by the registered nurse responsible for the patient's care.
- All practitioners must be aware of the right of the patent to have access to the record and give careful consideration to the language and terminology used.

Computer held records

- Health records held on computer must only be available to those authorised to access, through the application of role based access controls, to avoid the risk of breaching confidentiality
- there are access controls to restrict users of the system to specific functions as defined by the system manager.
- screens are not to be left unattended when the system is active.
- Include local procedures as to how entries into the computer records are authenticated in the absence of a written signature, each entry must clearly indicate the identity of the originator of the record.

Storage of health records

- All health records held in the hospices are safeguarded against loss, damage, or use by unauthorised persons by keeping health records in secure controlled locations at all times; locked rooms, locked cabinets or security protected computer systems.
- Authorised personnel have 24-hour access to the stored health records.
- All health records are kept for a minimum period of 10 years *(see the CHC Records Retention Schedule for details).*

Archiving paper patient records

- When paper records are archived, they must be stored in an archiving locked filing cabinet or box.

- Items stored in an archiving box must be clearly identified on its label, along with the department/manager responsible and date at which the contents of the box can be destroyed.
- Archiving boxes will only be stored in identified secure controlled locations. The period of time for records to be retained will vary; detailed information relative to retention periods is provided in the 'Cornwall Hospice Care Records Retention Schedule'. This schedule is not exhaustive, if there is any doubt as to how long an item should be archived, the Information Governance Officer should be asked.

Destruction of health records

- Health records are destroyed once they have been retained beyond the period defined within the 'CHC Records Retention Schedule'.
- Records are destroyed in such a way as to ensure that confidentiality is not breached This will usually be by shredding the entire content of the record if paper or by deleting the content of records held on electronic media.
- When there are large quantities of paper patient records to be destroyed (e.g. after an annual review determining which records should be destroyed) the maintenance team should be contacted to arrange for the contracted company to remove and securely destroy the records.
- Where records are incinerated by an external company, the process is monitored and the company is required to give a written 'Certificate of Destruction'.

Staff training requirements

- All care staff will be made aware of this policy and procedure and be aware of professional guidance on record keeping for clinical staff.
- Staff responsible for health records management will have had training in the provisions of the GDPR and Data Protection Act 2018.

All personnel working within the health records service have specific induction and update training including training on patient/user confidentiality and on the security of records, including electronic patient records.

Audit plan

Regular and on-going audit of the content, completeness and security of patient health records the results of which are compiled into a report to the Quality Assurance and Clinical Services Committee within the hospices.

Legal Status of the Health Record

Any document which records any aspect of care of a patient/service user can be required as evidence before a court of law, the Parliamentary Proceedings Committee or a professional conduct committee.

The health record is a confidential document whether in writing or electronic format. Access to it is therefore restricted but it should be available to all members of the multi-professional care team that do, or are likely to, deliver direct healthcare to the patient.

The originator must ensure that entry made in a record is complete and accurate and based on respect for truth and integrity and is not just an opinion.

Requirements that Apply Generally

The patients NHS number will be the primary unique identifier for each patient.

Completion of the record: All members of the multi-professional care team are responsible for keeping records of their interventions with patients.

The purpose of the health record is to:

- provide accurate, current, comprehensive and concise information concerning the condition and care of the patient, including details of consultations and the wishes and preferences of the patient and carers;
- provide a baseline record against which improvement or deterioration may be judged;
- provide a record of any problems that arise and the action taken in response to them;
- provide evidence of care required, interventions carried out and patient responses;
- include a record of any factors (physical, psychological or social) that appear to affect the patient;
- record patient-defined outcomes of treatment and care to inform quality management activities;
- record the chronology of events and the reasons for any decisions made.

Clinical Information Assurance

Data quality is crucial and the availability of complete, accurate, relevant and timely data is important in supporting patient/service user care, governance, management and service agreements for health care planning and accountability. It is therefore important all employees dealing with health records recognised the importance of data quality and their responsibilities.

Definitions

- **Data:** Data is a collection of facts from which information is constructed via processing or interpretation.
- **Information:** Information is the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.

- **Data Quality:** Data quality is a measure of the completeness, appropriateness, accuracy and timeliness of the data collected

General Principle of data quality. Good data quality should be:

- Accurate (values captured, as far as known to be true at point of entry, i.e. checking of demographic by asking the service user)
- Appropriate
- Complete (mandatory fields within documented procedures must be completed, i.e. postcode, GP Surgery)
- Consistent (data should be consistent with national codes where applicable and should be synchronised across systems)
- Defined
- Timely (data should be recorded as near to the event as possible)

Ensuring a high level of data quality of the CHC's clinical database (paper or electronic) is essential for the following reasons:

- Any duplication of patient records can result in medical notes being split across registrant records, and the risk that important information will be missed prior to patient consultation.
- Accuracy for activity reporting for management, clinical commissioning group (CCG) and national submissions (Minimum Data Set – The National Council for Palliative Care). For example, incorrect or missing GP details can result in error reporting for CCG's.
- Incorrect patient organisation links can result in information being transferred to the wrong organisation (i.e. nursing homes, GP). Minimised risk here is important to avoid confidentiality breach.
- Incorrect patient address/contact can result in delays in care and the possibility of information being sent to an incorrect address which would result in a breach of confidentiality.
- Delays in clinical entries can affect the patient safety for other services involved. All entries of clinical data for the use of direct care should be completed within 24 hours from the event. See excerpt from NMC Code in Appendix C, GMC Good Record Practice exert in Appendix D and HCPC Standards of conduct, performance and ethics in Appendix E.

It is the responsibility of all users of clinical information to ensure accurate, timely and appropriate data with compliance to relevant process documentation.

Sending Electronic Patient Data

Sending of patient data/information electronically must be done with the strictest confidentiality. The following must be considered in reference to the data being sent:

- Is there just enough for the recipient to identify the patient?
- Is the receiving source secure?
- Has the right amount of information been sent?
- Has the information/patient ID been double checked before being sent?

Once you have fulfilled the above you must consider where the information is going. If this is being sent via a CHC email/ NHS email account with the recipient also having a CHC email/NHS email account, the information does not have to be encrypted. However, as NHS accounts are many the recipient should be double checked to ensure correct person/address.

If the information is going from a secure CHC email/NHS account to a non-secure account (e.g. most nursing homes) then the IT Team should be contacted to arrange a secure means of sending these emails.

Faxing patient information is still necessary at times. Such incidences as faxing prescriptions, care plans and referrals to external sources is still common practice, although are being phased out by many health establishments. The following guidance is being used by the NHS and will form the protocol for CHC:

a) Does it need to be faxed?
b) Is it urgent? Is it better to have a conversation about this?

General Guidance:

c) Try to site fax machines away from public areas
d) Send faxes to named individuals if at all possible. 'Mark them addressee only'
e) Only send patient identifiable information by fax when absolutely necessary. Use identity numbers (e.g. NHS number) or initials if they will suffice.
f) Do not send more information than required for the purpose.
g) Check the fax number is correct-use pre-programmed numbers where possible.
h) Try to call recipient to inform them that the fax is about to be sent. Ask them to acknowledge receipt of the fax. If they do not call you, try and call them again.
i) Use the CHC fax cover sheet only which contains PRIVATE and CONFIDENTIAL and contact numbers.

Transportation of Confidential Records

For full details for transporting confidential records see the 'CHC Transportation of Health Records Procedure', but note:

- If an inpatient is travelling from the hospice to attend an appointment at Royal Cornwall Hospital Trust and we need them to carry their notes with them we

must ensure the notes are secure any patient notes carried by the patient will have to be in a sealed envelope.

Lost or misplaced patient information:

- If any document or file is misplaced, an immediate search must be conducted to locate it. If it is not found at once, this should be reported immediately to the appropriate line manager (i.e. the manager in whose area the document was last known to be held): the line manager must instigate appropriate efforts to locate and retrieve the material.
- If a document, file or data is known to be lost or stolen, or if it has not been located by action taken under the preceding paragraph, the Director of Education and Governance/Director of Patient Services must be advised immediately, or in her absence, the Director of Finance as Senior Information Responsible Officer (SIRO and DPO).
- Lost or stolen health records is an information security breach and the process at Appendix A should be followed and an Incident form completed (Appendix B)

What to do when an error occurs

If there is a breach of confidentiality or lost/stolen records an incident form must be completed. Any incidents relating to Data Protection /confidentiality issues must be notified to the line manager, service lead and Caldicott Guardian on the same working day. Each situation will be assessed on a case by case basis with the support of your manager.

Patients need to be advised of what has happened, unless it is detrimental to their health needs. Always seek advice first from the Caldicott Guardian.

If records are kept with the patient at home and the patient dies the records must be retrieved by the relevant department as soon as is reasonably possible.

If a relative or carer discloses that they have disposed of or destroyed the records a note should be made on the base record and the Caldicott Guardian informed and an incident form completed on the same span of duty.

Service leads and line managers are required to provide patients equal access to their health care records as outlined in this policy, making reasonable adjustments where required. Any discriminatory incidents in relation to this policy adversely impacting on the equal opportunities protected characteristics should be reported using the incident reporting system.

Staff must complete an incident form if the standards for managing the quality of health records in this policy are not up held.

All record keeping incidents and near misses must be reported to the Director of Education and Governance.

The Clinical Incident Forum will review and monitor any clinically related information governance breaches and escalate them when appropriate. This is important if they identify any error or anomaly within a record they are handling e.g. an error in recording patient identification details or health care information inserted into the wrong health records.

The aim of reporting incidents is to make timely improvements to information quality by providing a record of issues that can be addressed rather than wait for a record keeping audit.

Continuous quality improvements demonstrate the importance staff place on the accuracy, safety and storage of patient information recorded in health records.

If a breach is found to be serious this may result in the disciplinary procedure being implemented which could result in dismissal.

Compliance

This policy supports compliance with:

a. Care Quality Commission requirements under the Health & Social Care Act 2008 (Regulated Activities) Regulations 2010
b. Health & Social Care Act 2008 (regulated Activities) Regulations 2010
c. Data Protection Act 2018
d. General Data Protection Regulations
e. Access to Health Records Act 1990
f. Records Management – NHS Code of Practice
g. Nursing & Midwifery Council – www.nmc.org.uk/standards
h. General Medical Council – Good Medical Practice. www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/good-medical-practice
i. Health & Care Professions Council – Standards of conduct, performance and ethics – www.hcpc-uk.org/aboutregistration/standards/standardsofconductperformanceandethics
j. Misuse of Drugs Regulations 2001

Process for Monitoring Effective Implementation

This policy will be reviewed every three years by the Clinical Governance Committee, or more frequently if recommended practice or regulations require it.

The effectiveness of this policy will be monitored through exception reporting by the Caldicott Guardian and the Clinical Quality Assurance Group.

Training, Education & Development Required

All staff accessing records will receive training in the application of this Policy and underlying principles and practice as it applies to their particular roles. This will include:

- Using CHC record systems;
- Confidentiality, security and Information governance requirements (mandatory training).

Associated Documents

CHC Governance Policy

CHC Organisational Information and Records Policy

CHC Subject Access Requests – including Access to Health Records Policy and Procedure

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

CHC Data Protection Policy

Appendix A – Information Incident Reporting

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 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.

Appendix B – Information Incident Reporting Form

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:

Appendix C - Code of Conduct NMC Accurate Record Keeping Exert

Keep clear and accurate records relevant to your practice

This includes but is not limited to patient records. It includes all records that are relevant to your scope of practice.

To achieve this, you must:

- complete all records at the time or as soon as possible after an event, recording if the notes are written sometime after the event
- identify any risks or problems that have arisen and the steps taken to deal with them, so that colleagues who use the records have all the information they need
- complete all records accurately and without any falsification, taking immediate and appropriate action if you become aware that someone has not kept to these requirements
- attribute any entries you make in any paper or electronic records to yourself, making sure they are clearly written, dated and timed, and do not include unnecessary abbreviations, jargon or speculation
- take all steps to make sure that all records are kept securely, and
- collect, treat and store all data and research findings appropriately.

Appendix D - GMC Good Medical Practice Record your work clearly, accurately and legibly Exert

Record your work clearly, accurately and legibly

Documents you make (including clinical records) to formally record your work must be clear, accurate and legible. You should make records at the same time as the events you are recording or as soon as possible afterwards.

You must keep records that contain personal information about patients, colleagues or others securely, and in line with any data protection requirements.[14]

Clinical records should include:

a. relevant clinical findings

b. the decisions made and actions agreed, and who is making the decisions and agreeing the actions

c. the information given to patients

d. any drugs prescribed or other investigation or treatment

e. who is making the record and when.

Appendix E - HCPC Standards of conduct, performance and ethics - Keep records of your work Exert

Keep records of your work

Keep accurate records

You must keep full, clear, and accurate records for everyone you care for, treat, or provide other services to.

You must complete all records promptly and as soon as possible after providing care, treatment or other services.

Keep records secure

You must keep records secure by protecting them from loss, damage or inappropriate access.