Policy and Procedure: Health Records: Management of Patient Records
Policy number: 4.2

1. Policy Statement

Hospice in the Weald is committed to 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 legal and national requirements and safeguarded against damage, loss or improper usage.

2. Related policies, guidelines and procedures

4.1	Patient Access to Health Records
4.9	Health Records Information Sharing
8.11	Clinical Research
12.1	Information Communication Technology (ICT)
8.15	Disciplinary Procedures

3. Responsibility and Accountability

Policy formulation and review:	Emma Allwright, Head of Care Records
Clinical Approval:	Helen McGee, Medical Director
Compliance:	All staff and volunteers

4. Relevant Dates

Policy originated:	July 2004
This Review Date:	May 2018
Next Review Date:	May 2021

5. Procedure: Aim and Scope

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, security and destruction of health records.

6.   *Staff Responsibilities*

- Medical Director

  Responsible for ensuring that health records are adequately maintained for all patients   Responsible for ensuring this policy and procedure is in place and adhered to.

- Caldicott Guardian

  Responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that the Hospice satisfies the highest practicable standards for handling patient identifiable information.

- Registered Manager

  Responsible for ensuring that the content of the policy and procedure is in line with statutory 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 of the policy through the provision of suitable information materials (e.g. Patient Handbook).

- Clinical staff

  Responsible for compliance with the policy and procedure

- Information Governance Officer/Information Security Manager

  Responsible for the implementation and enforcement of the Information Security Policy in conjunction with this policy and procedure. The Hospice Information Governance Officer/Information Security Manager is the Head of Facilities/ICT.

7.   *Creation of Health Records*

- All health records are kept securely on EMIS, our Electronic Care Record (ECR) database. Each patient is allocated a unique patient number which is recorded on all documentation relating to that patient. This and their demographic details are recorded on the ECR which forms their electronic record.

- Patient documentation is also scanned directly into the patients ECR, using the following for identification:

  ∗   patient number
  ∗   date of documentation
  ∗   who the document is from i.e. Consultant, Specalist Nurse, Scan Type etc.

- All paper health records are kept securely in the Hospice archive.

- Durng a ward stay some paper notes will be kept i.e. Medication charts. Where appropriate these will be scanned into the patients ECR and then shredded. If the documents cannot be scanned these will be stored in the archive.

8. Completion of Health Record

All members of the multi-professional care team are responsible for keeping records of their interventions with patients in order 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, social or spiritual) that appear to affect the patient.
- Record the chronology of events and the reasons for any decisions made.

9. Electronic Care Records (ECR)

Hospice in the Weald uses electronic health records (ECR) provided by EMIS as the main health record. All ECR entries must adhere to the following principles:

- Be password protected to avoid the risk of breaching confidentiality.
- Be clear and unambiguous.
- If abbreviations are used these **MUST** be in line with the agreed acronyms **(Click here for the Abbreviation List).**
- All practitioners must be aware of the right of the patient to have access to the ECR and give careful consideration to the language and terminology used.

10. Storage of Electronic Care Records[1]

To ensure security of these records the following **MUST** be in place:

- Access controls to restrict users of the system to specific functions as defined by the Clinical Department Manager and the Information Security Manager.
- Screens are not to be left unattended when the system is active in the health records system, unless they are locked.

11. Amendment of Electronic Care Records

- Amendments can be made directly to the clinical record.
- All amendments can be tracked on the audit module on EMIS.
- If an amendment is made, this can be tracked via an audit tool. If the staff member cannot amend the record then an email needs to be sent to carerecords@hospiceintheweald.org.uk.

12. Destruction of Electronic Records

- Digitally held records are not destroyed but are archived on the ECR system.

13. Paper Health Records

If entries are made in paper records (medication charts), these must be:

- Written legibly in black ink
- Clear and unambiguous
- Dated
- Timed
- 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, if used these **MUST** be in line with the agreed acronyms **(Please click here to view the Abbreviation List).**

- Alterations are made by scoring out with a single line, so that the original entry can still be read alongside the correction and then initialled. Liquid paper, adhesive paper or tipp-ex must not be used to delete an 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.

14. Storage of Paper Health Records[1]

- All health records held in the hospice are safeguarded against loss, damage, or use by unauthorised persons by keeping health records in secure controlled locations at all times.   Authorised personnel have 24-hour access to the stored health records.

- All health records are kept for a minimum period of 10 years.

- All records relating to the research activity will be maintained accurately and stored for 5 years or, in the case of those involving drug trials, 15 years.

15. Duplicate Records

These are only created at the request of the Medical Director or Registered Manager either for legal purposes or for patients/relatives requesting access to their notes (see policy 4.1 Patient Access to Health Records).

16. Destruction of Paper Health Records

- Health records are destroyed once they have been retained beyond the statutory retention period.
- 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 held or by deleting the content of records held.

17. Legal status of the Health Record

- Any document which records any aspect of care of a patient 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 (ECR) form. Access to it is therefore restricted but it should be available to all members of the multi professional care team.

- The originator must ensure that any entry made in a health record is accurate and based on respect for truth and integrity.

18. Staff Training Requirements

All care staff are to be aware of the policy and procedure and be aware of professional guidance on record keeping for clinical staff.

All clinical staff will have had training in the provisions of the GDPR, as part of their annual Mandatory Training.

19. Audit Plan

Adherence to the stated policy will be audited through:

- Regular and on-going audit of the content and completeness of patient health records, the results of which are compiled into a report to the Clinical Governance group within the Hospice.

20. References

1. Storage of Health Records – Please refer to the document Part 2 Annex D1 (Health records retention schedules) at the following link on the Department of Health website: http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

21. Other References

- Access to Health Records Act 1990: http://www.legislation.gov.uk/ukpga/1990/23/contents

- Code of Professional Conduct for Nurse Midwife and Health Visitor (2015): http://www.nmc.org.uk/standards/code/

- Good Medical Practice (2013) – Keeping Records: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/good-medical-practice/domain-1---knowledge-skills-and-performance#paragraph-19 (accessed 24.5.18)

- A Clinician's Guide to Record Standards, Academy of Medical Royal Colleges, July 2013: https://www.aomrc.org.uk/wpcontent/uploads/2016/05/Standards_for_the_Clinical_Structure_and_Content_of_Patient_Records_0713.pdf (accessed 24.5.18)

- Royal College of Physicians. Generic medical record keeping standards. June 2015 https://www.rcplondon.ac.uk/resources/generic-medical-record-keeping-standards (accessed 24.5.18)

- NHS Records Management code of practice: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga (accessed 24.5.18)

- Guide to the General Data Protection Regulation (GDPR): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (accessed 24.5.18)