



Integrated Health Records Policy Access, Management, and Data Sharing

4.01

Document control sheet

Integrated Health Records Policy Access, Management, and Data Sharing

Document Detail

Document type	<i>Policy</i>
Document name	<i>Integrated Health Records Policy Access, Management, and Data Sharing</i>
Internal / external	<i>Internal and External</i>
Document location	<i>Hospice Web</i>
Version	<i>1.0</i>
Effective From	<i>06/03/2025</i>
Review date	<i>06/03/2028</i>
Policy owner	<i>Paul Madden, Director of Care Service</i>
Lead author	<i>Paul Madden, Director of Care Service</i>
Additional author(s)	<i>John Davison, Operations Director at BLS</i>
Applies to	<i>All staff and volunteers involved in handling health records within Hospice in the Weald.</i>
Approved by, date	<i>Information Governance Sub-Committee, March 2025</i>

Change History

Date	Change details since Approval	Approved by
<i>03/01/2025</i>	<i>New policy amalgamating 4.01, 4.02, and 4.09 with update-to-date information and guidance provided by BLS.</i>	<i>Information Governance Sub-Committee</i>
<i>20/05/2025</i>	<i>Addition in information sharing for staff to use NHS email when sharing outside of Hospice in the Weald</i>	

Contents (*amend page numbers as required*)

Document Control Sheet	
Change History	1
Document Summary Sheet	3
1. Overview	4
2. Scope	4
3. Associated Documents	4
4. Key terms - abbreviations & definitions	5
5. Policy	5
5.3. Health Records: Management of Patient Records	6
5.4. Patient Access to Health Records	9
5.5. Health Records: Data Sharing	11
6. Roles & Responsibilities	15
7. Monitoring Effectiveness	15
8. References	16
9. Guidance for the Policy Co-ordinator	16
10. Equality impact screening tool	17

Document Summary Sheet

Key Information

This document outlines the principles, standards, and procedures for the management, access, and sharing of health records at Hospice in the Weald. Below are the key points:

- **Confidentiality**
All health records must be securely stored and accessed only by authorised personnel, in compliance with UK GDPR and the Data Protection Act (2018) (<https://www.gov.uk/data-protection>)
- **Accuracy**
Health records must be complete, contemporaneous, and accurately reflect patient care.
- **Patient Access**
Patients and their legal representatives have the right to access their health records, with requests processed within one month.
- **Retention and Destruction**
Health records must be retained according to the NHS Records Management Code of Practice and securely destroyed after the statutory retention period.
- **Data Sharing**
Records may only be shared with patient consent, for lawful purposes, or in the public interest, following the Access to Health Records Act (1990) and Health and Social Care Act (2012).
- **Training**
All staff and volunteers handling records must complete annual training on data protection and record-keeping.

Compliance Highlights

- **Legal Frameworks**
This policy aligns with UK GDPR, the Data Protection Act (2018), the Mental Capacity Act (2005), and other relevant legislation.
- **Cybersecurity**
Electronic health records (ECR) must be password-protected, and access is logged and audited for security.
- **Roles and Responsibilities**
Specific roles, including the Caldicott Guardian and Data Protection Officer, are outlined for managing data confidentiality and compliance.

Key Procedures

- **Health Record Management**
 - Use the EMIS system for all electronic records.
 - Paper records, where used, must be scanned into the system and securely destroyed.
- **Patient Requests**
 - Requests must be logged and processed within one month, ensuring compliance with legal and ethical guidelines.
 - Third-party disclosures require explicit consent or lawful justification.
- **Monitoring and Audits**
 - Regular audits and training sessions ensure ongoing compliance and highlight areas for improvement.

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 3 of 18
---	----------------------------	---------------------	-------------------------------	---------------------

1. Overview

This policy outlines the principles, responsibilities, and procedures for the access, management, and sharing of health records at Hospice in the Weald. It ensures compliance with all relevant legal and regulatory frameworks, including:

- The UK General Data Protection Regulation (GDPR), as supplemented and tailored by the Data Protection Act (DPA) 2018, which governs the processing of personal data in the UK post-Brexit.
- The Access to Health Records Act 1990, which provides specific guidance for accessing records of deceased individuals.
- The Health and Social Care Act 2012, which introduces additional requirements for health data sharing and patient information governance.
- The Equality Act 2010, ensuring inclusivity and accessibility for all patients, including those with disabilities.
- Guidance from the Care Quality Commission (CQC) on record-keeping and information sharing.
- The Mental Capacity Act 2005, ensuring appropriate handling of records for individuals with diminished or fluctuating capacity.

The aim of this policy is to safeguard patient information, maintain accurate and comprehensive records, and enable appropriate data sharing to support high-quality, person-centred care. It ensures that health record management practices respect patients' rights, uphold confidentiality, and comply with all statutory and professional obligations.

If you have any concerns about the content of this document, please contact the policy owner or advise the Policy Coordinator via policy.coordinator@hospiceintheweald.org.uk

2. Scope

This policy applies to all staff and volunteers involved in handling health records within Hospice in the Weald. It encompasses electronic and paper-based health records, including:

- Adult and children's services
- Data sharing with external organisations
- Records of deceased patients

3. Associated Documents

- ICT Policy (12.01)
- Consent Policy (3.01)
- Safeguarding Vulnerable Adults (6.01)
- Disciplinary Procedures (8.15)
- Data Protection Policy (6.10)

4. Key terms - abbreviations & definitions

GDPR	General Data Protection Regulation
DPA	Data Protection Act (2018)
ECR	Electronic Care Record
MCA	Mental Capacity Act (2005)
CQC	Care Quality Commission
SAR	Subject Access Request
EMIS	Egton Medical Information Systems
NCSC:	National Cyber Security Centre

Caldicott Guardian - A senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate data sharing.

5. Policy

This policy defines the rules, principles, and standards for the access, management, and sharing of health records at Hospice in the Weald. It ensures compliance with all relevant legal and regulatory frameworks while safeguarding patient confidentiality and supporting high-quality care.

5.1. Principles Governing Health Records

5.1.1. Confidentiality

- All health records, whether electronic or paper-based, must be securely stored to prevent unauthorized access.
- Access is restricted to authorised personnel and must comply with UK GDPR and the Data Protection Act (2018) - <https://www.gov.uk/data-protection>
- Patient confidentiality must be respected at all times, and data must only be shared when there is a lawful basis, valid consent, or a public interest requirement.

5.1.2. Accuracy and Completeness

- Health records must be accurate, comprehensive, and completed in a timely manner to ensure they provide a clear account of care provided.
- Amendments must be transparent and made in a manner that preserves the integrity of the original entry.
- Regular review and weeding of health records should be undertaken to ensure their ongoing accuracy, relevance, and compliance with organisational policies and legal requirements.

5.1.3. Access to Records

- Patients have the right to access their health records, primarily under UK GDPR, which provides a broader right of access than the Access to Health Records Act (1990).
- Requests for access will be handled promptly, within statutory timeframes, and supported by secure processes to verify identity.

5.1.4. Retention and Destruction

- Records must be retained in accordance with the NHS Records Management Code of Practice.
- Secure methods, such as shredding or data deletion, must be used to destroy records that are no longer required after their statutory retention periods.

5.1.5. Data Sharing

- Sharing of patient data must be guided by explicit patient consent or a lawful basis such as safeguarding, public interest, or legal obligations.

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 5 of 18
---	----------------------------	---------------------	-------------------------------	---------------------

- Third-party disclosures must adhere to strict confidentiality protocols.
- Staff sharing any information outside of Hospice in the Weald must use encrypted NHS email.

5.2 Procedures for Implementation

5.2.1 Creation of Health Records

- All records are maintained electronically in the EMIS system, ensuring a unique patient identifier for each record.
- Paper records used in specific instances, such as during hospice stays, must be scanned into the system and securely destroyed.

5.2.2. Documentation Standards

- All entries must include the date, time, name, and designation of the individual making the entry.
- Abbreviations must be consistent with organisational standards and clearly defined on first use.
- Records must reflect accurate observations, interventions, and decisions to provide a comprehensive record of patient care.
- While records can be updated or annotated, staff must not go back and alter or delete original entries, ensuring the integrity and transparency of the record.

5.2.3. Access Requests

- Requests for health records can be submitted in writing, electronically, verbally, or via social media, in accordance with UK GDPR. Verification of the requester's identity and authorisation is required to process all requests.
- Records of deceased patients will only be released to personal representatives or individuals with a legal claim under the Access to Health Records Act (1990).

5.2.4. Data Security

- Electronic systems must be password-protected, and screens locked when unattended.
- Paper records must be stored in secure, controlled-access areas.
- When sharing information outside of Hospice in the Weald NHS encrypted email must be used.

5.2.5. Training and Education

- Staff and volunteers must receive training on data protection, record management, and security protocols.
- Training will include specific guidance on responding to patient requests and handling sensitive information.

5.3. Health Records: Management of Patient Records

5.3.1. Creation of Health Records

All health records are maintained securely on the EMIS Electronic Care Record (ECR) system, ensuring each patient is assigned a unique identifier to prevent duplication and ensure traceability.

Patient documentation, such as consultation notes and external correspondence, must be scanned into the ECR system with the following details clearly recorded:

- patient number
 - date of documentation
 - Originator (i.e. Consultant, Specialist Nurse, Scan Type etc.)
- All paper health records are kept securely in the Hospice archive.
 - During a Ward or Cottage Hospice 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.

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 6 of 18
---	----------------------------	---------------------	-------------------------------	---------------------

- The Children's Service may leave paper notes in the family home, for example a drug chart and any supporting documentation around drug dosages and regimes. This will be kept in a plastic wallet and labelled the property of Hospice in The Weald, with contact details of the Children's Service. Once a drug chart is no longer in use it will be scanned onto EMIS and the paper copy shredded.

5.3.2. 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.
- Registered staff at Cottage Hospice will be required to complete electronic EMIS records on patients for interventions carried out during every shift as above, in an accurate and contemporaneous manner.
- The Children's Service will complete electronic EMIS records after each session of care. Records must be complete, consistent, and consecutive. Unregistered staff will undertake record keeping training. Registered staff are accountable for the delegated task and must regularly review notes and ensure entries meet the required standards.

5.3.3. 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 and written in full for the first time.
- 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.

5.3.4. Storage of Electronic Care Records

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.

5.3.5. 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.
- Amendments must be transparent and made in a manner that preserves the integrity of the original entry.
- Regular review and weeding of health records should be undertaken to ensure their ongoing accuracy, relevance, and compliance with organisational policies and legal requirements.
- 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

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 7 of 18
--	---------------------	--------------	------------------------	--------------

5.3.6. Destruction of Electronic Records

- Digitally held records are archived on the ECR system in line with the NHS Records Management Code of Practice retention schedule.
- Records that have exceeded the specified retention period and are no longer required must be securely destroyed to ensure compliance with legal and regulatory standards.
- According to the NHS Records Management Code of Practice 2021, adult health records should be retained for 8 years after the conclusion of treatment or the patient's death. The British Medical Association (BMA) also provides guidance on the retention of health records, stating that in England and Wales, records should be retained for 10 years after a patient's death. Therefore, HitW will adopt the BMA's recommendation.

5.3.7. 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.
- 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 patient to have access to the record and give careful consideration to the language and terminology used.

5.3.8. Storage of Paper Health Records

- 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 maximum period of 10 years post treatment or death (following the BMA guidelines).
- Children's records are kept until they reach the age of 25, or 26 if the young person was 17 when treatment ended, or 8 years after the child or young person has died.
- 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.

5.3.9. Duplicate Records

These are only created at the request of the Clinical Director or Registered Manager either for legal purposes or for patients/relatives requesting access to their notes (5.4. Patient Access to Health Records)

5.3.10. Destruction of Paper Health Records

- Health records are destroyed once they have been retained beyond the statutory retention period.

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 8 of 18
--	---------------------	--------------	---------------------------	--------------

- Records are destroyed in such a way as to ensure that confidentiality is not breached. This process typically involves shredding the entire content of paper records or securely deleting the content of electronic records.
- Whether destruction is conducted internally, or outsourced, robust monitoring arrangements must be in place to ensure that records are securely destroyed in compliance with organisational policies and regulatory requirements, including guidance from the Information Commissioner's Office (ICO).

5.3.11. 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.

5.4. Patient Access to Health Records

5.4.1. Receiving the Access Request & Checking the appropriate access request details

Any request for access to health records can be made in writing, electronically, verbally, or via social media in accordance with UK GDPR. Requests should be forwarded to the Caldicott Guardian, who is the Clinical Director, or in their absence, to the Care Director.

In cases where consent is given verbally or through social media, the details of the consent, including the method and content of the request, must be documented clearly in the individual's Care Record to ensure transparency and compliance with organisational policies.

Once a subject access request is received, the consent of the applicant must be verified by ensuring:

- Full name -including previous names
- Full address -including previous address (es).
- Hospice Number and/or NHS Number (optional).

If a patient's representative, i.e. solicitor, is applying for access, ensure the Hospice has the signature of the patient to do this.

Once a child/ young person reaches the age of 16, they are presumed by law to be competent to give consent for themselves or ask for access to their own health records, if they are not competent then it will be the person with parental responsibility.

Once a child or young person reaches the age of 16, they are presumed by law to be competent to give consent for themselves or request access to their own health records. For data protection purposes, however, children aged 13 and above are also considered capable of consenting to the processing of their personal data, including access to their health records. If a young person is not competent, the responsibility will fall to the individual with parental responsibility.

Within Children's Services, consent will typically be obtained from the parent or legal guardian, who holds parental responsibility for the child or young person. However, for data protection purposes, children aged 13 and above are generally considered competent to provide consent for the processing of their personal data, including decisions related to their health records. Where the child or young person is not deemed competent, consent will revert to the person with parental responsibility.

5.4.2. Fees to access and copy health records

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 9 of 18
---	----------------------------	---------------------	-------------------------------	---------------------

- In most cases we cannot charge a fee to comply with an access request. However, where the request is excessive, we may charge a “reasonable fee” for the administrative costs of complying with the request.
- We can also charge a reasonable fee if an individual requests further copies of their data following a request.
- The fee must be based on the administrative costs of providing further copies. However, this decision needs to be explained to the individual.

Once the fee has been received then the Hospice can release the copies.

5.4.3. Logging and actioning the Access Request

- Requests, once documentation is complete, should be complied and returned to the data subject with within one month.
- Once the request is logged, this should be passed to the Caldicott Guardian. At Hospice in the Weald, this is the Director of Clinical Excellence. The Caldicott Guardian will read through the notes and advise on which sections of the notes are to be released (see Denying Access below). If the Director of Clinical Excellence is absent from the Hospice, the Head of Hospice Outreach Service will act in their place.

5.4.4. Denying Access

Access should be denied if consent has not been obtained.

Records, or part of records, are not to be released to a patient or the person with legal responsibility for them, if it is felt that by its release, it may cause serious physical or mental harm to the individual to whom the data refers, or another person.

- It is likely to cause serious physical or mental harm to the patient or another person
- It relates to a third party who has not given consent for disclosure (where the third party is not a health professional who has cared for the patient)
- It is requested by a third party and the patient had asked that the information be kept confidential
- The records are subject to legal professional privilege
- It is restricted by order of the courts
- If the request is unfounded or excessive
- If the patient has given explicit instruction not to disclose information to another party even after they have died

Any withheld information should be redacted or blocked out, but this decision must be justified.

If we refuse to comply with a request, we must inform the individual within one month of receiving the request, fully explaining the reasons why the request has been refused and outlining their right to appeal to the ICO.

5.4.5. The Release Stage

On the release of the records, where the information is not readily intelligible, an explanation (e.g. of abbreviations or medical terminology) must be given.

If it is agreed that the patient or their representative only wishes to view their health records, this should be supervised by a health professional or a lay administrator. In these circumstances the lay administrator must not comment or advise on the content of the record and if the applicant raises enquiries, an appointment with a health professional should be offered.

5.4.6. Third Party Disclosure

Where records contain information that relates to an identifiable third party (this could be a healthcare professional or informal carer or relative etc) that information may not be released unless:

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 10 of 18
---	----------------------------	---------------------	-------------------------------	----------------------

In relation to healthcare professionals,

- The third party has compiled or contributed to the health records or who has been involved in the care of the patient e.g. “was told by Dr that there were no further treatment options”. If the entry is accusatory or derogatory in any way the healthcare professional should be informed that this information is being released.

In relation to informal carers, relatives etc.

- The third party, who is not a health professional, gives their consent to the disclosure of that information.

If consent has not been satisfied from details about any third party contained within the patient’s health records, then information should still be disclosed without revealing the identity of the third party. This can be done by omitting names and identifying particulars from the records and care should be taken to ensure that the information, if released is genuinely anonymous.

5.4.7. Deceased Patients

Unless they requested confidentiality while alive, a patient’s representative and any other person who may have a claim arising out of the patient’s death has a right of access to information in the deceased person’s records directly relevant to a claim. No information that is not directly relevant to a claim should be disclosed to either the personal representative or any other person who may have a claim arising out of the patient’s death.

- Information will only be disclosed to a nominated representative of the deceased once they have provided suitable documentary evidence, such as proof of their legal status or authority to act.
- The Access to Health Records Act (1990) only applies to the release of health records and does not extend to other types of personal information.
- A necessary and proportionate approach should be applied to disclosures, ensuring that only relevant information is provided. Certain details, such as third-party information, may be redacted to maintain confidentiality where appropriate.

5.4.8. Amendments to Health Records

- UK GDPR includes the right to rectification. This gives patients the right to have inaccurate data rectified or completed if incomplete. A request for rectification needs to be made in writing or verbally.
- If amendments are to be made these need to be done within one month of receiving the request. If a patient feels that information recorded on their health record is incorrect, then they should firstly make an informal approach to the health professional concerned to discuss the situation in an attempt to have the records amended. Amendments to records must be made in a way which indicates why the alteration was made so that it is clear that records have not been tampered with.
- Patients may also seek correction of information they believe is inaccurate. The health professional is not obliged to accept the patient’s opinion but must ensure that the notes indicate the patient’s view. A copy of the correction or appended note should be given to the patient.
- If the patient is still dissatisfied, they may pursue a complaint under the Hospice complaints procedure, Adverse Comments and Complaints (6.4) June 2017, in an attempt to have the information corrected or erased.

5.5. Health Records: Data Sharing

5.5.1. Information sharing

All staff should maintain confidentiality when dealing with requests for information about patients. Any requests from third parties (outside of the Hospice where this is not the patient themselves) should be discussed with the Director of Clinical Excellence (or, in her absence, the Director of Care Services) and the following guidelines adhered to.

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 11 of 18
--	---------------------	--------------	---------------------------	---------------

Failure to follow this guidance may result in disciplinary action in accordance with the Hospice's Disciplinary Policy.

5.5.2. Disclosing information with consent

Ideally this should be in writing (this may be in the form of a letter or email, which will be scanned into the Electronic Care Record); where it is not, the consent should be witnessed and recorded on the Electronic Care Record.

The Data Protection Act 2018 provides specific legal bases for the sharing of health data, including the necessity for medical purposes or substantial public interest. Data sharing agreements should clearly state these legal bases

Seeking a patient's consent to disclosure of information shows respect and is part of good communication between care professionals and patients.

Most patients understand and accept information must be shared within the healthcare team in order to provide their care. You should make sure information is readily available to patients explaining that, unless they object, personal information about them will be shared to support the provision of their care.

You must make sure that anyone you disclose personal information to understands that you are giving it to them in confidence, which they must respect. All staff members receiving personal information in order to provide or support care are bound by a legal duty of confidentiality, whether or not they have contractual or professional obligations to protect confidentiality.

Circumstances may arise in which a patient cannot be informed about the disclosure of information, for example in a medical emergency. In such a case you should pass relevant information promptly to those providing the patient's care. If and when the patient is capable of understanding, you should inform them how their personal information was disclosed if it was in a way they would not reasonably expect.

You must respect the wishes of any patient who objects to particular information being shared within the healthcare team or with others providing care, unless disclosure would be justified in the public interest. If a patient objects to a disclosure that you consider essential to the provision of safe care, you should explain you cannot refer them or otherwise arrange for their treatment without also disclosing that information.

5.5.3. When required by law

The Data Protection Act 2018 allows for processing of personal data where required by law, including regulatory investigations or public health purposes, provided such processing complies with the Act's principles. In certain situations, we have to release information about a patient because we are required in law to do so. Such situations include, but are not limited to:

- When the recipient has approval to receive it under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002. This allows the Secretary of State for Health or the Health Research Authority to set aside the common law duty of confidentiality in special circumstances including improving patient care or in the 'public interest'.
- Satisfy a specific statutory requirement, such as notification of a known or suspected case of certain infectious diseases.
- When some regulatory bodies have statutory powers to access patients' records as part of their duties to investigate complaints, accidents or health professionals' fitness to practice. Many regulatory bodies have codes of practice governing how they will access and use personal information. For example, a Form 172 (Authority to Disclose details of Medical conditions and treatment relevant to an offence).

Whenever practicable, you should inform patients about such disclosures, unless that would undermine the purpose, even if their consent is not required.

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 12 of 18
---	----------------------------	---------------------	-------------------------------	----------------------

You must disclose information if ordered to do so by a judge; but should object to the judge if attempts are made to compel you to disclose what appears irrelevant. You must not disclose personal information to a third party such as a solicitor, police officer or officer of a court without the patient's express consent unless it is required by law or can be justified in the public interest.

5.5.4. In the public interest

In limited circumstances there may be a public interest in disclosing information in order to protect individuals or society from risks of serious harm, such as communicable diseases, crime and safeguarding from abuse.

Personal information may be disclosed in the public interest, without patients' consent, and in exceptional cases where patients have withheld consent, if the benefits to an individual or to society outweigh both the public and the patient's interest in keeping the information confidential.

Before considering whether a disclosure of personal information would be justified in the public interest, you must be satisfied that identifiable information is necessary for the purpose, or that it is not reasonably practicable to anonymise or code it. In such cases, you should still seek the patient's consent unless it is not practicable to do so, in which case the next of kin, family, carer or guardian may be approached.

You may consider not seeking consent when there is a risk of harm to self in doing so or if in seeking consent you would prejudice the purpose of the disclosure – e.g. an investigation into a safeguarding issue.

You must document in the patient's record your reasons for disclosing information without consent and any steps you have taken to seek the patient's consent, to inform them about the disclosure, or your reasons for not doing so.

5.5.5. After a patient's death

Your duty of confidentiality continues after a patient has died. Whether and what personal information may be disclosed after a patient's death will depend on the circumstances. If the patient had asked for information to remain confidential, you should usually respect their wishes. If you are unaware of any instructions from the patient, when you are considering requests for information, you should take into account the impact on the family and whether any disclosure can be anonymised; this will depend on the reason for the disclosure.

You are required to disclose relevant information about a patient who has died, for example:

- to help a coroner, or other similar officer, with an inquest or fatal accident inquiry
- when disclosure is required by law, is authorised under section 251 of the NHS Act 2006, or is justified in the public interest, such as for education or research
- for National Confidential Inquiries or for local clinical audit
- on death certificates, which you must complete honestly and fully
- for public health surveillance, in which case the information should be anonymised or coded, unless that would defeat the purpose
- when a partner, close relative, or friend asks for information about the circumstances of an adult's death, and you have no reason to believe that the patient would have objected to such a disclosure, and when a person has a right of access to records under the Access to Health Records Act (1990) rather than under the General Data Protection Regulation 2018.

Archived records relating to deceased patients remain subject to a duty of confidentiality.

5.5.6. Local clinical audit

If an audit is to be undertaken by the team that provided care, or those working to support them, such as clinical audit staff, you may disclose identifiable information, provided you are satisfied that the patient:

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 13 of 18
---	----------------------------	---------------------	-------------------------------	----------------------

- a) has ready access to information that explains that their personal information may be disclosed for local clinical audit, and that they have the right to object, and
- b) has not objected.

If a patient does object you should explain why the information is needed and how this may benefit their own, and others' care. If it is not possible to provide safe care without disclosing information for audit, you should explain this to the patient and the options open to them.

If clinical audit is to be undertaken, but not by the team that provided care or those who support them, the information should be anonymised or coded. If this is not practicable, or if identifiable information is essential to the audit, you should disclose the information only if you have the patient's express consent.

5.5.7. Disclosures for which express consent should be sought

As a general rule, you should seek a patient's express consent before disclosing identifiable information for purposes other than the provision of their care or local clinical audit, such as financial audit and insurance or benefits claims.

If you are asked to provide information to third parties, such as a patient's insurer or employer or a government department or an agency assessing a claimant's entitlement to benefits, either following an examination or from existing records, you should:

- a) be satisfied that the patient has sufficient information about the scope, purpose and likely consequences of the examination and disclosure, and the fact that relevant information cannot be concealed or withheld
- b) obtain or have seen written consent to the disclosure from the patient or a person properly authorised to act on the patient's behalf; you may accept an assurance from an officer of a government department or agency or a registered health professional acting on their behalf that the patient or a person properly authorised to act on their behalf has consented
- c) only disclose factual information you can substantiate, presented in an unbiased manner, relevant to the request; so you should not usually disclose the whole record, although it may be relevant to some benefits paid by government departments and to other assessments of patients' entitlement to pensions or other health-related benefits, and
- d) offer to show your patient, or give them a copy of, any report you write about them for employment or insurance purposes before it is sent, unless:
 - i) they have already indicated they do not wish to see it
 - ii) disclosure would be likely to cause serious harm to the patient or anyone else
 - iii) disclosure would be likely to reveal information about another person who does not consent.

5.5.8. Sharing information with a patient's partner, carers, relatives or friends

You should establish with the patient what information they want you to share, who with, and in what circumstances. This will be particularly important if the patient has fluctuating or diminished capacity or is likely to lose capacity, even temporarily. Early discussions of this nature can help to avoid disclosures patients would object to. They can also help to avoid misunderstandings with, or causing offence to, anyone the patient would want information to be shared with.

If a patient lacks capacity and unless they previously indicated otherwise, it is reasonable to assume that patients would want those closest to them to be kept informed of their general condition and prognosis. If anyone close to the patient wants to discuss their concerns about the patient's health, you should make it clear to them that, while it is not a breach of confidentiality to listen to their concerns, you cannot guarantee that you will not tell the patient about the conversation. You might need to share with a patient, information you have received from others, for example, if it has influenced your assessment and treatment of the patient.

You should not refuse to listen to a patient's partner, carers or others on the basis of confidentiality. Their

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 14 of 18
---	----------------------------	---------------------	-----------------------------------	----------------------

views or the information they provide might be helpful in your care of the patient. You will, though, need to consider whether your patient would consider you listening to the concerns of others about your patient's health or care to be a breach of trust, particularly if they have asked you not to listen to particular people.

5.5.9. Data Sharing Patient ECR's with GP's

Our ECR package allows us to data share with Medical Practices that use the same package. This data sharing works in both directions we can see GP entries against shared patients as well the GP's being able to see Hospice entries. To enable data sharing the appropriate GP Practice must sign a data sharing agreement which is then forwarded onto the ECR Package provider and is switched on. Under the UK General Data Protection Regulations (UK GDPR), the Hospice uses the lawful basis of 'Legitimate interests' to share patient's data. Data is only shared with other Health Care Professionals. Before a member of staff can access a record from another provider, the reason for this must be noted on the ECR. Every time a shared record is viewed, an audit trail is made of who accessed the notes, at what time and the reason documented.

6. Roles & Responsibilities

6.1. Staff with people management responsibilities

- Ensure that their teams comply with the policy and related procedures.
- Provide necessary training and resources to staff for effective record management and data protection.
- Monitor and address any non-compliance within their teams, implementing corrective actions as required.
- Support audits and reviews of health record practices and implement changes based on findings.

6.2. Staff and volunteers

- Adhere to the guidelines outlined in the policy and any associated procedures.
- Ensure the confidentiality, accuracy, and security of health records they handle.
- Complete mandatory training on data protection, record-keeping, and data-sharing practices.
- Promptly report any data breaches or concerns regarding health records to their line manager or the Information Governance Lead.

6.3. Caldicott Guardian / Deputy Caldicott Guardian

- Oversee the confidentiality of patient records and ensure compliance with legal and regulatory requirements.
- Review and approve data-sharing requests and disclosures where necessary.
- Provide guidance on ethical and legal considerations related to record management.

7. Monitoring Effectiveness

7.1. Key standards

- Record Accuracy: All patient records must be complete, accurate, and contemporaneous for 100% of care episodes.
- Timely Documentation: 100% of patient interactions should be documented in the EMIS system within 24 hours of the event.
- Training Completion: 100% of staff and volunteers handling records must complete data protection, cyber security, and records management training annually, at a level appropriate to their role, in accordance with the updated requirements of the Data Security and Protection Toolkit (DSPT).
- Access Compliance: All subject access requests must be processed within one month, per statutory requirements.

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 15 of 18
--	---------------------	--------------	---------------------------	---------------

7.2. Method(s)*:

- Audits: Regular audits of patient records will ensure compliance with documentation and storage standards.
- Training Records: Attendance logs and completion rates for mandatory training programs will be reviewed.

7.3. Responsibility for Monitoring

The Information Governance Lead and the Caldicott Guardian will be responsible for monitoring compliance with this policy.

7.4. Frequency of Monitoring

Compliance will be monitored quarterly through audits of patient records, data-sharing activities, and staff training completion rates. Additionally, annual reviews will be conducted to evaluate overall adherence to this policy and any changes in legal or regulatory requirements.

7.5. Process for Reviewing Results and Ensuring Improvements in Performance

Monitoring results will be compiled into compliance dashboards, which will be shared with the teams involved and reported to the Executive Team Quarterly. Quarterly summaries will be presented to the Governance and Risk Committee, with actionable recommendations to address any identified gaps.

8. References

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Access to Health Records Act 1990
- Mental Capacity Act 2005
- Health and Social Care Act 2012
- Equality Act 2010
- NHS Records Management Code of Practice
- Care Quality Commission (CQC) Guidance
- National Institute for Health and Care Excellence (NICE) Guidelines
- National Cyber Security Centre (NCSC) Recommendations
- NHS England Patient Safety Alerts

9. Guidance for the Policy Co-ordinator

Must be fully completed by the author prior to publication.

Keywords & phrases	Health Records Policy, Data Protection, UK GDPR Compliance, Access to Health Records, Patient Confidentiality, Electronic Care Records (ECR), Data Sharing Guidelines, Record Retention and Destruction, Mental Capacity Act, Record-Keeping Standards
Document review arrangements	Review will occur by the author, or a nominated person, within three years or earlier should a change in legislation, best practice, or other change in circumstance dictate.
Special requests	All Services staff and volunteers should be made aware of this policy.

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 16 of 18
--	---------------------	--------------	------------------------	---------------

10. Equality impact screening tool

- This screening tool must be completed at the start of any new or existing policy or procedure development. All sections of the tool will expand as required.

Section 1			
Protected Characteristic	If the proposal/s have a positive or negative impact, please give brief details		
Age	Positive - The policy ensures equitable access to health records for all age groups, with additional considerations for children and young people.		
Disability	Positive - Accessibility features for patients with disabilities, such as clear communication formats, are supported.		
Gender reassignment	Neutral - No specific impact identified beyond ensuring confidentiality and equality of access.		
Marriage or civil partnership	Neutral - No specific impact identified beyond compliance with legal standards.		
Pregnancy and maternity	Neutral - No specific impact identified beyond safeguarding patient confidentiality and data security.		
Race	Positive - Translation services are available to support individuals for whom English is not a first language.		
Religion or belief	Neutral - No specific impact identified.		
Sex	Neutral - No specific impact identified.		
Sexual orientation.	Neutral - No specific impact identified beyond maintaining confidentiality.		
Other underserved communities (Including Carers, Low Income,	Positive - Specific provisions ensure that carers can access necessary health records when authorised.		
Section 2			
Will implementation of this policy / procedure have a <u>significant</u> adverse impact for people with protected characteristics or otherwise listed above, in relation to <u>any</u> of the following six categories? Please mark in the yes/no checkbox below, as appropriate. NB: In this context 'significant' means that potential adverse impacts of implementing the policy can <u>not</u> be mitigated against within the policy / procedure itself. - Adversely affect patient safety or clinical effectiveness - Adversely affect compliance with statutory/regulatory requirements e.g. NICE requirements, CQC, Equality Act, Care Act etc. - Adversely affect the experience of a patient or their loved one(s) - Adversely affect the experience of staff or volunteers - Adversely affect access to Hospice services			
Yes		No	
High risk: Complete further Equality Impact Assessment (EqIA) tool, available from the Policy Co-ordinator policy.coordinator@hospiceintheweald.org.uk	☐	Low risk: Go to section 3.	☒
Section 3			
If this proposal is low risk, please give evidence or justification for how you reached this decision: This policy has been assessed as low risk because it upholds confidentiality, promotes equitable access to records, and is designed to support compliance with relevant statutory and regulatory requirements. There are no identified adverse impacts for individuals with protected characteristics or underserved groups.			
Title: Integrated Health Records Policy Access, Management, and Data Sharing		Policy Number: 4.01	Version: 1.0
		Issue Date: 18/04/2025	Page 17 of 18

Signed by Policy Lead Author	Paul Madden (Director of Care Services)	Date	17 th January 2025
-------------------------------------	---	-------------	-------------------------------

Title: Integrated Health Records Policy Access, Management, and Data Sharing	Policy Number: 4.01	Version: 1.0	Issue Date: 18/04/2025	Page 18 of 18
---	----------------------------	---------------------	-------------------------------	----------------------