**Document Details**

<table>
<thead>
<tr>
<th>Title</th>
<th>Clinical Record Keeping Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Ref No</td>
<td>1545-53879</td>
</tr>
<tr>
<td>Local Ref (optional)</td>
<td>Version 1.8</td>
</tr>
<tr>
<td>Main points the document covers</td>
<td>The policy sets out the arrangements to achieve good clinical records keeping practice, in line with legislative and regulatory standards and national guidance and requirements</td>
</tr>
<tr>
<td>Who is the document aimed at?</td>
<td>All staff</td>
</tr>
<tr>
<td>Owner</td>
<td>Alan Ferguson, Records Manager &amp; Quality Facilitator</td>
</tr>
</tbody>
</table>

**Approval process**

| Who has been consulted in the development of this policy? | The Records Manager consulted with representatives from services and departments across the organisation through the Records Management Group and with relevant specialist staff and clinical and administrative leads. |
| Approved by (Committee/Director) | Records Management Group on behalf of the Information Governance Operational Group |
| Approval Date | 2nd July 2019 |
| Initial Equality Impact Screening | Yes |
| Full Equality Impact Assessment | No |
| Lead Director | Steve Gregory, Director of Nursing and Operations |
| Category | General |
| Sub Category | Information Governance |
| Review date | 1st July 2021 |

**Distribution**

| Who the policy will be distributed to | All staff |
| Method | Publication on the Trust Intranet, Records management training, |
| Keywords | Records, record keeping, records manager, Caldicott Guardian, clinical, clinical systems, electronic patient records, EPR, RiO, paper records, health records, patient held records, creation, use, archiving, tracking, transfer, disposal, destruction, verification, information quality, data protection, subject access request, scanned records, scanning, digital, digital records, information governance, data security and protection toolkit, NHS Number, unique identifier, consistent identifier, record, patient record, clinical record, records management, retrieval, verification, use, systems, quality, adopted persons, transgender persons, witness |
Introduction

Legal Obligations

Purpose

Definitions

A Record

Records Management:

Duties

The Chief Executive

Directors, Deputy Directors and Senior Managers

The Director of Nursing and Operations

The Deputy Director of Nursing and Quality

Records Manager

Local Records Management Leads

Caldicott Guardian

Information Governance Manager

Managers and Team Leaders

Staff

Temporary Staff

Document Links

Required by CQC

Yes

Other

Data Security and Protection Toolkit (DSPT)

Amendments History

<table>
<thead>
<tr>
<th>No</th>
<th>Date</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>May 2012</td>
<td>Previous PCT Policy reviewed and updated to reflect the organisational structure of Shropshire Community Health NHS Trust and the latest regulatory requirements.</td>
</tr>
<tr>
<td>2</td>
<td>Aug 2013</td>
<td>Changes to contact details for the Information Governance and Data Protection Lead</td>
</tr>
<tr>
<td>3</td>
<td>Nov 2014</td>
<td>Review and minor updates to reflect organisational changes and links to reference information</td>
</tr>
<tr>
<td>4</td>
<td>Mar 2017</td>
<td>Review and minor updates to reflect organisational changes and links to reference information</td>
</tr>
<tr>
<td>5</td>
<td>June 2019</td>
<td>Updated to reflect changes in Data Protection Legislation (DPA 2018 &amp; GDPR) and review of record keeping processes in particular to bring guidance in line with the use of the new Electronic Patient Record system (RIO). This policy now incorporates the previous separate “NHS Number Retrieval Verification and Use Procedure”</td>
</tr>
</tbody>
</table>

Contents

1 Introduction ................................................................................................................................. 4
2 Legal Obligations ....................................................................................................................... 4
3 Purpose ........................................................................................................................................ 4
4 Definitions ................................................................................................................................... 5
4.1 A Record ................................................................................................................................. 5
4.2 Records Management: .......................................................................................................... 5
5 Duties ........................................................................................................................................ 5
5.1 The Chief Executive ............................................................................................................ 5
5.2 Directors, Deputy Directors and Senior Managers .......................................................... 5
5.3 The Director of Nursing and Operations .............................................................................. 6
5.4 The Deputy Director of Nursing and Quality ....................................................................... 6
5.5 Records Manager .................................................................................................................. 6
5.6 Local Records Management Leads .................................................................................... 6
5.7 Caldicott Guardian ............................................................................................................... 7
5.8 Information Governance Manager ..................................................................................... 7
5.9 Managers and Team Leaders ............................................................................................... 7
5.10 Staff ...................................................................................................................................... 8
5.11 Temporary Staff ................................................................................................................... 8
<table>
<thead>
<tr>
<th>Appendix</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tracking</td>
<td>24</td>
</tr>
<tr>
<td>17</td>
<td>Retrieval of Paper Records</td>
<td>25</td>
</tr>
<tr>
<td>18</td>
<td>Movement of Paper Records</td>
<td>25</td>
</tr>
<tr>
<td>18.1</td>
<td>Taking Paper Records off site</td>
<td>25</td>
</tr>
<tr>
<td>18.2</td>
<td>Labelling and Packaging of Records for Transporting</td>
<td>26</td>
</tr>
<tr>
<td>18.3</td>
<td>Electronic Records</td>
<td>26</td>
</tr>
<tr>
<td>19</td>
<td>Storage of Paper Records</td>
<td>26</td>
</tr>
<tr>
<td>20</td>
<td>Mobile and Homeworking</td>
<td>27</td>
</tr>
<tr>
<td>21</td>
<td>Retention and Disposal</td>
<td>27</td>
</tr>
<tr>
<td>22</td>
<td>Records Audit</td>
<td>27</td>
</tr>
<tr>
<td>22.1</td>
<td>Clinical Record Keeping Audit</td>
<td>28</td>
</tr>
<tr>
<td>23</td>
<td>Consultation</td>
<td>28</td>
</tr>
<tr>
<td>24</td>
<td>Dissemination</td>
<td>28</td>
</tr>
<tr>
<td>25</td>
<td>Advice</td>
<td>28</td>
</tr>
<tr>
<td>26</td>
<td>Training</td>
<td>29</td>
</tr>
<tr>
<td>27</td>
<td>Review</td>
<td>29</td>
</tr>
<tr>
<td>28</td>
<td>Compliance Monitoring</td>
<td>29</td>
</tr>
<tr>
<td>29</td>
<td>Related Documents</td>
<td>29</td>
</tr>
<tr>
<td>30</td>
<td>References</td>
<td>30</td>
</tr>
<tr>
<td>31</td>
<td>Glossary</td>
<td>30</td>
</tr>
<tr>
<td>31.1</td>
<td>Definitions</td>
<td>30</td>
</tr>
<tr>
<td>31.2</td>
<td>Abbreviations</td>
<td>32</td>
</tr>
<tr>
<td>Appendix 1</td>
<td>Record Keeping Related Legislation, National Standards and Requirements</td>
<td>34</td>
</tr>
<tr>
<td>Appendix 2</td>
<td>Example Records Register</td>
<td>39</td>
</tr>
<tr>
<td>Appendix 3</td>
<td>Example Tracer Card</td>
<td>40</td>
</tr>
<tr>
<td>Appendix 4</td>
<td>Example Clinical Document Format and Layout</td>
<td>41</td>
</tr>
<tr>
<td>Appendix 5</td>
<td>Clinical Record Keeping Audit planning</td>
<td>42</td>
</tr>
<tr>
<td>Appendix 6</td>
<td>Clinical Record Keeping Audit Form Template - example</td>
<td>46</td>
</tr>
</tbody>
</table>
1 Introduction

Clinical record keeping is an integral part of professional practice, designed to inform all aspects of the care process. The use of patient information is an essential aspect of any NHS organisation and is a key element in supporting the everyday aspects of the delivery of high quality, evidence based health care.

Accurate and effective clinical record keeping is fundamental to high quality patient/client care. It also enables effective communication with other professionals involved in patient/client’s care and expresses individual professional accountability and responsibility. It is important that these records are accurate, up to date and easily accessible to those who need to use them. This policy also addresses record keeping issues and recommendations raised during inquiries such as the “Inquiry into care provided by Mid Staffordshire NHS Foundation Trust” – the Francis Report.

2 Legal Obligations

Any document (hard copy or electronic), which records any aspect of the care of a patient or client, can be required as evidence before a court of law or before Preliminary Proceedings Committee of the Professional Councils. All NHS health care records are the property of NHS and not the health care professional or patients / clients. Health records are public records and are “owned” by the Secretary of State and must be kept in accordance with legal and professional obligations set out in the Records Management Code of Practice for Health and Social Care in addition to the following legislation and any new guidance affecting records management as it arises:

- The Public Records Act 1958
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The NHS Confidentiality Code of Practice

3 Purpose

The purpose of this policy is to establish the systematic and planned approach to the management of clinical records to ensure that, from the moment a record is created until its ultimate disposal, Shropshire Community Health NHS Trust (SCHT) maintains information so that it serves the purpose it was collected for and disposes of the information appropriately when no longer required. This policy covers both hard copy and electronic records. The standards and best practice guidance applies to staff working in all patient care settings, including community clinics, community hospitals, care homes and prisons, patient’s homes/place of residence.

This policy is specifically intended to ensure that the Trust meets its obligations in respect of clinical record keeping. However, in doing so, it recognises that the Trust works closely with partner organisations and agencies in the provision of services. This is particularly relevant where services are provided under joint working arrangements where health and social care staff work together in a single management structure. The terms of this policy are intended to apply to all staff.
working in such environments and who are contributing to clinical records for which the Trust is responsible.

4 Definitions

4.1 A Record

The ISO standard, ISO 15489-1:2016 Information and documentation - Records management defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'.

The Data Protection Act 2018 (DPA) defines a health record which 'consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual'.

4.2 Records Management:

The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records [BS ISO 15489-1:2001].

For additional records management related definitions please see the Glossary section.

5 Duties

The Records Management Code of Practice for Health and Social Care has been published by the Information Governance Alliance (IGA) for the Department of Health (DH) and is a guide for use in relation to the practice of managing records. It is relevant to organisations who work within, or under contract to NHS organisations in England. This also includes public health functions in Local Authorities and Adult Social Care where there is joint care provided within the NHS. It is based on current legal requirements and professional best practice

5.1 The Chief Executive

The Chief Executive has overall responsibility for records management in the Trust. As the accountable officer they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

5.2 Directors, Deputy Directors and Senior Managers

Directors, Deputy Directors, Divisional and Service Managers of units and business functions within the Trust have overall responsibility for the management of records generated by their activities i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust’s records management policies.
5.3 The Director of Nursing and Operations
The Director of Nursing and Operations acts as the lead director for records management within the Trust.

5.4 The Deputy Director of Nursing and Quality
Operational responsibility for records management is assigned to the Deputy Director of Nursing and Quality, who manages the Records Manager.

5.5 Records Manager
Operational responsibility is assigned to the Trust’s Records Manager. The Records Manager is therefore responsible for:

- Chairing the Trust's Records Management Group
- Assisting directorates and services to achieve good record keeping and compliance with the relevant standards, legislation, policies and procedures relating to the management of records
- Reporting to the Deputy Director of Nursing and Quality, on areas where improvements could be made and the resources required
- Ensuring that records management audits are conducted by directorates and services
- Acting as Caldicott Support and liaising with, and supporting, the Caldicott Guardian to ensure that the records management activities are in line with national and local guidance and protocols on confidentiality
- Liaising with the Information Governance Manager in records management related issues, initiatives and support requirements
- Liaising with, and supporting, the Corporate Risk Manager in records management related incidents investigations and follow up actions
- Advising and supporting the activities of the Local Records Management Leads
- Liaising with the Local Records Management Leads, other relevant staff leads, and the Organisations Development team to ensure staff receive appropriate records management training
- Encouraging all staff to follow the policies, procedures, guidance and best practice on records management

5.6 Local Records Management Leads
Local Records Managers have been identified to represent directorates and services within the Trust. Services that do not have Local Records Managers must ensure that Local Records Administration Leads are in place to take responsibility for the required records management processes. Where no Local Records Administrative Lead has been identified the Local Team Leader will take on this responsibility.

Local Records Managers and / or Local Records Administration Leads are responsible for ensuring that the following are implemented for all records in their directorate or service:

- Processes for the monitoring of local records management activities and supporting staff in records related issues
- Records registration, maintenance and tracking systems
• Systems for the safe storage and retention of records
• Records are archived in appropriate, secure areas
• Retention periods guidance as defined in the Records Management Policy, Records Retention section are followed
• A mechanism for identifying records which must be permanently kept
• Secure and Confidential means to dispose of records when required
• Supporting the reporting and investigation of records management related incidents
• Identify areas of concern in the management of records and, when necessary, bring these topics for discussion by the Records Management Group
• Conduct / support relevant audits of local record keeping practices / procedures
• Advising on the training requirements of their staff, including local induction training

5.7 Caldicott Guardian
The Caldicott Guardian is responsible for approving and ensuring that appropriate protocols for the management of confidential patient information are in place. In particular they are responsible for monitoring compliance with Trust’s Confidentiality Code of Conduct. The Trust’s Director of Nursing and Operations acts as its Caldicott Guardian.

5.8 Information Governance Manager
The Information Governance Manager acts as the Trust’s Lead for Information Governance and is the Trust’s Data Protection Officer. They are also chair of the Information Governance Operational Group.

5.9 Managers and Team Leaders
All Managers and Team Leaders are responsible for their staff and that local practices and procedures follow the principles set out in this policy. Their responsibilities include:
• Raising the profile of good record keeping practice
• Developing appropriate local induction / training programmes
• Ensuring staff attend the relevant Information Governance Records Management Mandatory Training as detailed in the Trust’s Mandatory Training Policy
• Monitoring the quality of record keeping, e.g. by peer review and audit
• Establishing adequate secure storage and tracking systems that allow prompt tracing and access to records held
• Ensuring compliance with relevant access legislation including; Data Protection and Freedom of Information
• Ensuring all staff are aware of their responsibility to maintain the confidentiality of patients and colleagues
5.10 **Staff**

All staff are responsible for:

- Any records that they create or use. This responsibility is incorporated into Professional Codes of Conduct e.g. Nursing and Midwifery Council (NMC) The Code 2015, Health and Care Professions Council (HCPC) Standards, Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in England and General Medical Council (GMC) Good Medical Practice: guidance for doctors
- Complying with the General Data Protection Regulations / Data Protection Act and related Data Protection Principles
- Keeping up to date with relevant training, best practice guidelines, policies, procedures and codes of practice
- Reporting any records related incidents following guidance given in the Trust's Incident Reporting Code of Practice

Under the Public Records Act 1958 the responsibility of the Chief Executive and senior managers for the safe keeping of records is extended to all staff for all records they either create, use or handle.

All staff who come into contact with patient or personal information are subject to a Common Law Duty of Confidentiality. This duty of confidence continues beyond the death of a patient or after an employee has left the NHS. The Data Protection Act principles should also be complied with.

This responsibility will be reflected in all job descriptions and assessed as part of staff appraisals.

5.11 **Temporary Staff**

Anybody undertaking work for or with the Trust such as bank or agency staff, locums or students must be advised about the Trust’s requirements for record keeping as part of their induction on arrival. It is the duty of the permanent staff handing care of patients to temporary staff to ensure that such staff are made aware of their responsibilities for record keeping.

5.12 **Information Governance Operational Group**

The Information Governance Operational Group will act as the forum for ensuring that compliance is achieved with the relevant legislative and regulative standards and will report through the Information Governance Framework to the Information Management & Technology Strategy Group / Quality and Safety Committee any issues of concern.

5.13 **Records Management Group**

The Records Management Group will provide a forum for Local Records Management Leads to discuss any records management topics and to support each other in day to day records management activities. This group is responsible for:

- Monitoring the implementation of this policy
- Monitoring clinical record keeping and related records audits
6 Confidentiality


6.1 Caldicott Principles

The Caldicott principles cover confidentiality and the protection and use of patient information. Each NHS organisation has a Caldicott Guardian to ensure the principles are implemented at local level. The Director of Nursing and Operations is the Trust’s Caldicott Guardian.

Staff must ensure they are aware of these principles. In brief they are:

- **Principle 1**: Justify the purpose(s) for using confidential information
- **Principle 2**: Don’t use personal confidential data unless absolutely necessary
- **Principle 3**: Use the minimum necessary personal confidential data
- **Principle 4**: Access to personal confidential data should be on a strict need-to-know basis
- **Principle 5**: Everyone with access to personal confidential data should be aware of their responsibilities
- **Principle 6**: Comply with the law
- **Principle 7**: The duty to share information can be as important as the duty to protect patient confidentiality

7 Informing Patients - Privacy Notice

Staff must explain to the patient, client or user any care or treatment they are planning on carrying out, the risks involved and any other treatments possible. They should also inform patients how the Service/Team will share their information with others as part of their direct care. Patients should be informed about the Trust’s Privacy Notice which gives them the relevant information about our purpose for collecting and using information about them.

8 Consent

Staff must make sure that they obtain and record the patient’s informed consent to any care or treatment they carry out. They must make a record of the agreed care or treatment decisions and pass this on to all members of the health or social care team involved in care. In emergencies, it may not be possible to explain treatment or get consent but the reasons for this not being possible should be...
recorded in their record and reasons for continuing to give care and treatment in the patient’s best interest.

The Mental Capacity Act (2005) states, as one of its statutory principles, that you must presume a person has capacity. If you have reason to believe that a person lacks capacity a formal assessment must be carried out and documented.

For further guidance on consent see the Trust’s Consent to Examination and Treatment Policy.

9 Records Lifecycle
The term “Records Life Cycle” describes the life of a record from its creation/receipt through the period of its active use, then into a period of inactive retention (such as closed files which may still be referred to occasionally) and finally confidential disposal or archival preservation. The key components of records management are:

- **Creation**: create and log quality information
- **Using**: use/handle
- **Retention**: keep/maintain in line with NHS recommended retention schedule
- **Appraisal**: determine whether records are worthy or Archival Preservation. Further use may be identified at this stage.
- **Disposition**: dispose appropriately according to Trust guidelines

It is imperative that records are closely monitored and managed throughout their lifecycle.

10 Clinical Record Keeping
Good record keeping is an integral part of professional practice and is essential to the provision of safe and effective care. It is not an optional extra to be fitted in if circumstances allow. As well as individual Professional Codes of Practice there are also national standards, legislation and regulations that must be met to ensure good clinical record keeping practice. These include:

- **Care Quality Commission**: Fundamental standards Regulation 17, Good Governance covers the record keeping requirements
- **Data Security and Protection Toolkit**: Information Governance covers the way organisations ‘process’ or handle information and includes both corporate and clinical information. The Data Security and Protection Toolkit (previously the Information Governance Toolkit) draws together the legal rules and central guidance and presents them in one place as a set of information governance requirements
- **Accessible Information Standard 2016**: Legislation to make sure that people who have a disability, impairment or sensory loss are provided with information that they can easily read or understand and with support so they can communicate effectively with health and social care services

For a brief overview of each of these see Appendix 1.

10.1 Record Keeping Functions
Good record keeping has many important functions. These include:
• Supporting patient care and communications
• Supporting the involvement of the patient in their own health care
• Supporting effective clinical judgements and decisions
• Promoting better communication and sharing of information between members of the multi-professional healthcare team
• Helping to identify risks, and enabling early detection of complications
• Supporting the delivery of services
• Helping to improve accountability
• Showing how decisions related to patient care were made
• Making continuity of care easier
• Providing documentary evidence of services delivered
• Supporting clinical audit, research, allocation of resources and performance planning
• Helping to address complaints or legal processes

10.2 Types of Clinical Records
The principles of good record keeping apply to all types of records, regardless of how they are held. Examples of records that should be managed using the guidelines are listed below. This list gives examples of functional areas as well as the format of the records:

• Patient health records (electronic or paper based, including those concerning all specialties and GP records)
• Records of private patients seen on NHS premises
• Accident & emergency, birth, and all other registers
• Theatre registers and minor operations (and other related) registers
• Administrative records (including, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling)
• X-ray and imaging reports, output and images
• Integrated health and social care records
• Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or for supporting commissioning decisions.

Format:
• Photographs, slides, and other images
• Microform (i.e. microfiche/microfilm)
• Audio and video tapes, cassettes, CD-ROM etc
• E-mails
- Computerised records
- Scanned records
- Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient) such as Twitter and Skype
- Websites and intranet sites that provide key information to patients and staff.
- Manual Records (such as case notes)
- Electronic Records (such as patient administration and clinical systems)
- Pictures and videos (Dicom images, ultrasound recordings)

10.3 Record Keeping Standards
Staff must keep clear, accurate and legible records, reporting the relevant clinical findings, the decisions made, the information given to patients, and any drugs prescribed or other investigation, care or treatment.

Clinical records must provide a safe and effective means of communication between appropriate members of the health care team - including the patient themselves. Where there are hard copy records, the location of all records must be recorded either on a clinical system or by using a records register (see example layout Appendix 2). It is important that all records are able to be identified and traced in order to provide prompt access to them when required.

Clinical records must:
- Be complete, consistent, accurate and consecutive
- Be factual and not include unnecessary abbreviations, jargon, meaningless phrases or irrelevant speculation.
- Only state relevant and useful information
- If abbreviations are used, they must be written in full the first time used e.g. Care Quality Commission (CQC) or from an approved abbreviation list. This approved abbreviation list must be held in any patient record they are used in
- Be recorded as soon as possible after an event has occurred, providing current information on the care and condition of the patient. This should be within 24 hours, if not, the reasons for the delay must also be recorded for any retrospective record keeping
- When the care being delivered to a patient has been delegated to an unregistered member of staff the registered member of staff is accountable for that patient and must ensure relevant entries are made in the patient record to reflect this
- Identify any risks or problems that have arisen and the action taken to rectify them
- Be recorded/written, wherever possible, with the involvement of the patient, carer or parent
- Be held securely and confidentially
The information contained within records must be used for the purpose for which it was obtained and only shared appropriately and lawfully.

In particular for hard copy records they must:

- Be written clearly, legibly and in such a manner that they cannot be erased.
- Be accurately dated, timed and signed (The signatory’s name must be printed at the side of the first entry or be matched to an authorised signatory list). The signatory’s designation / role must also be recorded (this can be alongside the signature or in a specific signature list held within the record).
- Erasers and liquid paper must not be used to cancel errors. A single line must be used to cross out and cancel mistakes or errors and this must be signed and dated by the person who has made the amendment.
- Be readable when photocopied or scanned.
- Be bound and stored so that loss of documents is minimised.

**Clinical records must not:**

- Include any coded expressions of sarcasm or humorous abbreviations to describe the patient/client.
- Be kept for longer than is necessary.

**Patient and Parent Held Records:** Where patients and / or parents hold their own, or their child’s, records they must be made aware of the importance of these records for health care professionals and the need to keep them safe. They must also be made aware that these records are an official health record and as such will need to be returned to the Trust when requested. With Community Nursing Patient Held Records they must have the contact details of the team delivering the care and treatment so that the record can be returned to that team when required. On completion of the care and treatment any hardcopy/paper Patient Held Records must be scanned and uploaded to the patient’s RiO Electronic Record. The record should scanned as a complete document.

### 10.4 Electronic Patient Record

With the introduction of the Trust’s Electronic Patient Record (EPR), using the RiO system, services have migrated from the current, mainly, paper records to the new electronic system where the individual patient record will be accessed by the relevant services delivering care to that patient. The record keeping practices detailed within this policy apply to both paper and electronic records and, as part of the transition to the new RiO system, processes and procedures will be put in place to ensure a consistent approach across the organisation while maintaining individual specialist requirements. The EPR Project Groups such as the Clinical Transformation Group and the Clinical Assurance Group will provide services with advice and guidance during this transition. This policy will continue to be reviewed to take into account new working practices and provide any additional guidance that is required. During this transition period it is important that operational clinical record keeping processes are
documented in the Service/Teams Standard Operating Procedures and that these follow Records Management best practice guidance.

10.5 Retrospective Record Keeping

Record Keeping best practice states that healthcare professionals should make records at the same time as the events they are recording or as soon as possible afterwards. However it is recognised that this is not always possible e.g. if the electronic record system is not available. In these cases an electronic document (e.g. Word) should be completed and saved at the time and then uploaded or copied into the patient’s record when next connected to the RiO system. A paper handwritten record should be the last option used and staff must ensure the information noted like this is entered into the patient RiO record as soon as possible and the paper note is confidentially destroyed. As part of service business continuity plans there may be paper versions of forms which should be used. These should be uploaded to the relevant patient RiO record once the system can be accessed.

If the record entry is late (being written in retrospectively) the progress note entry should be dated for the contact with the patient. The progress note entry should start with the date the notes were taken and brief reason for why there was a delay in entering them into RiO e.g. “written on <<date>> from notes taken at time due to unable to access RIO system” or “written on <<date>> as first opportunity to access records after clinics”. If someone has written an entry in the time between your contact and your writing up then use your judgement to decide if you need to take further action to keep them informed and ensure this is recorded.

10.6 Integrated Patient Record

Prior to the Electronic Patient Record System, RiO, individual services maintained their patient records but now the Trust have one electronic record where individual services and teams enter their information. This integrated patient record means that all those involved in the care and treatment of that patient will be aware of the activities of other Services and Teams. Care should be taken to maintain good record keeping practice to ensure other healthcare professionals are aware of relevant care and treatment being delivered by other services and teams and that there is no confusion with terminology or abbreviations used.

The Progress Notes should be used to inform others of the care and treatment being delivered and/or required but also to signpost others to areas of the electronic record such as forms that have been completed or documents that have been uploaded. The Progress Notes should be considered as the “golden thread” that leads others through the record.

10.7 Clinical Record Creation / Content

Records must provide a contemporaneous complete record of care. The contents of the record should be in a standardised structure and layout. The records must be completed with relevant information contained in chronological order, within the appropriate sections. In hard copy records, all items within a patient record should be attached securely i.e. they must not contain any loose documentation.
Clinical records must include:

- Registration/referral details of the patient. Information recorded must include: first name, last name, date of birth, NHS Number, address including post code, contact telephone number, gender, ethnicity, GP details and next of kin details. This information must be checked on first contact with the patient and then regularly to ensure it is up to date and accurate.

- Any communication requirements the patient may have, to ensure they receive information in the way they can access and understand.

- Medical referral details and related previous medical history.

- Any Alerts such as allergies or safeguarding.

- Medical observations: examinations, assessments, tests, diagnoses, prescriptions, other treatments.

- Other relevant information/forms/assessments such as Assessment of Capacity (Mental Capacity Act), Lasting Power of Attorney, Advanced Directives or Statements.

- Evidence of the care planned, risks assessed, the decisions made, the care delivered and the information shared.

- Evidence of actions agreed with the patient, including consent to care and treatment.

- Relevant disclosures by the patient – pertinent to understanding the cause or affecting the care/treatment of the illness.

- Details of facts and information given to the patient.

- Correspondence to and from the patient and/or other parties.

- Appropriate Discharge/Transfer of Care documentation.

It is important that all aspects of the record must be identifiable to the particular patient. In hard copy records every page must contain, at least, the following patient details:

- First Name
- Last Name
- NHS Number

This information must be in a consistent position throughout the record e.g. top left hand corner. Continuation sheets must be numbered so they can be identified and kept in chronological order.

10.8 Clinical Documentation

It is recognised that different services and specialities require specific documentation to meet their professional requirements but the Trust is keen to ensure a consistency in the documentation used across the whole organisation. With the introduction of the Electronic Patient Record System, RiO, the use of hard copy documents should be minimised and where possible relevant forms created with RiO so that information can be entered directly into the system. This not only makes it easier to enter the relevant information but
also means the information can be retrieved by use of reports within the system.

Where there is a requirement for a hard copy document to be created and used within patient records it must be approved and follow the Trust’s recommended layout and formatting (see Appendix 4 for example). The Records Manager will, liaising with the appropriate clinical leads and specialist staff, co-ordinate the design, review and approval of any clinical documentation, including any exceptions to the standard layout and formatting.

10.9 Local Record Keeping Processes

The Trust supports the move to the use of integrated records in order to have a comprehensive record of the patient’s care and promote better communication between clinicians and support safe effective care. Services are encouraged to review their record keeping processes and identify and implement integrated records where possible. The Managers and Local Team Leads of each service are responsible for ensuring the appropriate clinical record keeping processes are documented (e.g. as part of a Standard Operating Procedure) and implemented. The process must include:

- A brief overview of the service and its requirement to use clinical records, covering both paper and electronic where applicable
- The process for creating records including who is responsible for doing this
- Who is responsible for verifying that the patient details are correct e.g. demographic information including first name, last name and date of birth in order to verify the correct NHS Number
- What the standard record keeping process is for that Service/Team including any specific details of the use of progress notes and forms that should be used.
- How any incidents or concerns can be reported
- Who is responsible for monitoring the process and ensuring staff are aware of their responsibilities (in particular new or temporary staff)
- Who is responsible for dealing with any information sharing or Data Protection Subject Access Requests i.e. the Data Protection Liaison Officer (DPLO)

Even with the transition to the Electronic Patent Record system, RiO, there will still be a requirement to maintain and legacy paper records so any local process should include:

- How and where the record is stored and tracking processes that are in place
- Who is responsible for uploading any patient hard copy records to the patient’s electronic RiO Record on completion of their period of care and treatment or as required during their care and treatment
- How records are retrieved (include any out of hours requirements)
- How records are archived (including how the location of archived records are recorded)
10.10 Digital Media

It is recognised that the use of electronic devices such as Dictaphones, digital cameras and specialist medical equipment is a requirement in some services / departments within the Organisation. As these devices (and their output/media) may not be suitable for encryption, it is important that users consider the confidentiality and security of the information and reduce the risk of loss of any Personal Confidential Data (PCD).

When recording information on these devices full patient details should not be used. The use of an abbreviated identifier is recommended e.g. the patient’s initials and last four numbers of their NHS Number – AB7890. The identifier should be sufficient for other staff involved in the use of the information to link to the patient’s record but not for anyone else to be able to identify the person. Any tapes or separate recording media associated with these devices should be individually identifiable by that service/department e.g. tape SLT001, tape SLT002.

Digital media that needs to be retained specific to a patient should be labelled as with any other record and where practical included in the patient’s clinical record. A note of the existence of this digital media record should be made in the clinical notes. If the digital media cannot be stored with the clinical record a note of the storage location must be recorded in the notes.

10.11 Video Recording

As the Electronic Patient Record system (RiO) does not support video files, these should be stored on a secure local server and their location recorded in the Patient record. The saving of any video files should be carefully considered to justify the requirement i.e. for a specific clinical reason. A consent form detailing the reason for the use of the video and recording the relevant consent should be uploaded to the record. If the video is being used to write up an assessment or record observations then, once these records have been made the video file does not need to be retained unless there was a specific professional clinical reason to save it. Care should also be taken to ensure other children are not included in any recording without their specific consent.

The digital media should be treated as a clinical record and kept in accordance with relevant policies and guidelines including information security and records retention. Refer to the Information Security Policy for further guidance.

For specific advice reference digital photography of wounds please refer to the Clinical Photography Guidelines which give more detailed guidance covering the taking, printing and storage of the electronic images and printed copies of these images.

10.12 Scanned Records

With the implementation of the Trust’s Electronic Patient Record (EPR) system, RiO, there has been an increased need for paper documents to be scanned and uploaded to a patient’s record. In brief, it is important that during this process:

- all documents are scanned to a standard that they will be able to be opened and read on the EPR system
- the correct documents are uploaded to the correct patient’s records
these uploaded documents can then be found and retrieved by those who need to refer to them.

Where scanning is used, the main consideration is that the information can perform the same function as the paper counterpart did and like any evidence, scanned records can be challenged in a court. This is unlikely to be a problem provided it can be demonstrated that the scan is an authentic record and there are technical and organisational means to ensure the scanned records maintain their integrity, authenticity and usability as records, for the duration of the relevant retention period.¹

The legal admissibility of scanned records, as with any digital information, is determined by how it can be shown that it is an authentic record. An indication of how the courts will interpret evidence can be found in the civil procedure rules and the court will decide if a record, either paper or electronic, can be admissible as evidence.²

The actual process for scanning and uploading documents onto RiO will vary depending on the requirements and administrative processes defined by individual Services but the key principles should be the same. Services need to ensure that local processes are documented and all staff involved in the process understand the importance of taking care when scanning and uploading documents to ensure the right information is available in the right patient's records. Quality checks must be a part of these processes.

There are two stages to the process, one will be the scanning and/or preparing a document to be uploaded. This may involve the scanning of a paper copy of a document or the saving of an electronic file created or received. The second stage of the process is the actual uploading of the file to the patient's record in RiO.

**Scanning/preparing a document for upload:** It is important that any document being scanned and/or saved in readiness for uploading is saved using the file-naming convention of including the patient's name and NHS Number detailed in this section. This is so the file can be checked against the patient's name when in the upload screen in RiO.

**Uploading the document to RiO:** Once the document is ready to be uploaded to RiO the patient's record should be opened and the Document Upload option selected. When using the Browse function to find the saved file it is important that the filename is checked against the patient's details to ensure the document is being uploaded to the correct patient record.

**Disposal of Original Paper Documents:** Original paper copies of the document should not be destroyed until the scanning and quality checks have taken place and the system has gone through a back-up phase (for RiO, the back-up is carried out continually to a second server so data is backed-up at all times). Once a document has been scanned, uploaded and quality checked the uploaded copy of the document can then be considered as the primary

---


record and the, now secondary, paper original can be disposed of under confidential means. This disposal process should be included in local processes. Guidance on the time period will depend on any specific requirements within the Service but in most cases this can be done at the end of that day. It would not be expected for these secondary copies to be retained for longer than a week as there is a risk of a backlog building up and that these documents are not stored securely.

For further detailed guidance on Scanning and Uploading refer to the briefing paper “Scanning and Uploading of Documents” available, with other guidance documents, on the RiO User SharePoint Portal.

11 Patient Identification

All staff must be aware of the importance of the need for the positive identification of a patient before delivering care or treatment and during all stages of clinical treatment in order to ensure the matching of all elements of care, including notes, samples, specimens, medicines and surgical treatment, to the correct patient.

When asking a patient to confirm their details it is important you ask them to give you that information and not just agree to what you say e.g. “Can you please confirm your date of birth?” rather than “Is your date of birth 1 April 1970?”

12 NHS Number

Using the NHS Number as the national identifier for patients will significantly improve safety by ensuring patients are identified correctly. In clinical care the use of the NHS Number is of particular importance because it:

- Is the only National Unique Patient Identifier
- Supports safer identification practices
- Helps create a complete record, linking every episode of care across organisations

With the use of electronic systems and the need to improve clinical records management there is a need to ensure the linking of every episode of patient related care with the relevant NHS Number. Staff are therefore responsible for:

- Verifying the NHS Number of a patient / client at the start of an episode of care
- Ensuring that the patient / client is clearly identified on all care records, requests, referrals and results, using the NHS Number (recorded in a 3-3-4 format e.g. 123 456 7890)
- Promoting the use of the NHS Number

12.1 NHS Number Standard

The aim of the NHS Number Standard is to:

- Ensure that there is a means to create and maintain an accurate and reliable link between a patient/service user and the records of their care.
- Enable patient/service user records to be safely transferred across organisational boundaries.
- Facilitate electronic referrals and prescription activity.
- Facilitate requests and reports for tests and investigations.
- Accurately and safely identify patient/service users in all communications with tertiary, primary, secondary, community and social care teams.
- Help to create a complete record, enabling the linkage of every episode of care across organisations.
- Encourage or ensure the use of the NHS Number (where appropriate) and contribute to an improved service provider and receiver culture.

The general principles of the NHS Number standards are:

- **Find It** - find the NHS Number for a person as soon as possible in the care pathway, ideally on initial contact with the service.
- **Use It** - use the NHS Number to link a person to their care record; use the NHS Number to search for an electronic record; use the NHS Number on wristbands, documents and reports used for the care of the person.
- **Share It** - share the NHS Number with other organisations so they can use it; include the NHS Number on all correspondence and electronic messages.

12.2 Use of NHS Number in Sharing Information for Direct Care

Two new duties came in to force from 1 October 2015 as part of the Health and Social Care (Safety and Quality) Act. These are:

1. A requirement for health and adult social care organisations to use a consistent identifier (the NHS Number) for sharing data for direct care of a patient.
2. A legal duty requiring health and adult social care bodies to share information with each other for the direct care of a patient.

For a person's direct care, the default position should now be to share unless there is a reason not to. The Act aims to address the 'culture of anxiety' with regards to data sharing that was identified by the 2013 Caldicott Report.

12.3 Using the NHS Number

Staff working in NHS organisations, social care, and those contracted to provide services for the purposes of care e.g. opticians, pharmacists, dentists and audiologists, use the NHS Number to:

- Confirm and update patient demographic details.
- Synchronise patient demographic data with the NHS Spine
- Enhance patient safety by ensuring the right records are connected to the right patients.
- Accurately link the patient to their health records.
- Ensure safe and efficient coordination of social care with healthcare
- Make referrals using Choose and Book.
- Send electronic prescription messages.
- Transfer patient records electronically using GP2GP.
- Track patient test requests, results and outcomes.
• Identify patients in all communications with secondary and community care teams.
• Perform research and analysis.
• Support the contracting process including Payment by Results.

Staff are responsible for:
• Verifying the NHS Number of a patient / client at the start of an episode of care
• Ensuring that the patient/client is clearly identified on all care records, requests, referrals and results, using the NHS Number (in a 3-3-4 format e.g. 123 456 7890)
• Ensuring the patient’s NHS Number is used in all clinical correspondence
• Using the NHS Number for information sharing relating to the direct care of the patient

13 NHS Number procedure

13.1 Find It
Upon receipt of a referral, the referral should be recorded on the appropriate Electronic Patient Record / Clinical Information System(s) within 24 hours by the responsible staff member. If the patient is not already registered on the system, a registration must be recorded. If the patient is already registered on the system, all demographic details, including NHS Number, must be checked and validated against the data already recorded.

If the patient’s NHS Number is not provided on the referral letter, the member of staff taking responsibility for the referral must, in the first instance, contact the referrer to confirm the NHS Number.

Should the NHS Number not be available from the referrer, the member of staff must undertake a trace to ascertain the correct identifier for the patient. This trace should be undertaken within 3 working days. It is good practice to confirm all additional demographic information, including date of birth and GP. The Summary Care Record application (SCRa) should be used if tracing is not successful using other clinical systems. If still unsuccessful you should be report this to the Information Services department in order for them to investigate further.

13.2 Use It
Once obtained, the NHS Number must be recorded on the paper record and the appropriate Electronic Patient Record / Clinical Information System(s) by the responsible staff member. It must be used alongside the patient’s name (first and last) on each page in the paper record. This ensures that all pages of a record are identifiable back to the patient concerned.

In the Community Hospitals any patient identity band should clearly identify the patient’s name, date of birth and their NHS number, which is taken from, and corresponds with their patient record.

The Information Services Data Analysis Team will produce monthly reports on missing NHS Numbers. These will be disseminated to both administrative and
clinical staff, appropriate Senior Managers and the Records Manager. Each service must undertake follow up actions in order to rectify any issues identified and ensure any missing NHS numbers are updated. Any problems in resolving these issues should be reported back to the Records Manager and Clinical Information System Owners.

13.3 Share It
The sender of any clinical correspondence must ensure the patient’s NHS Number is a standard item of information included in any clinical patient documentation. Services referring, transferring or discharging patients must ensure the NHS Number is clearly recorded on the appropriate referral / transfer / discharge documentation.

Staff should raise the awareness of the use of the NHS Number with patients so that they can check that any clinical correspondence does relate to them. Patients can also use the NHS Number as a means of confirming details when arranging or attending consultations / appointments e.g. at GPs or Hospitals.

14 Additional NHS Number Guidance

14.1 Adopted Persons Health Records
Notwithstanding any other centrally issued guidance by the Department of Health and Social Services or the Department for Education, the records of adopted persons can only be placed under a new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used, but more commonly the birth names are used.

Depending on the circumstances of the adoption there may be a need to protect from disclosure any information about a third party. Additional checks before any disclosure of adoption documentation are recommended because of the heightened risk of accidental disclosure.

It is important that any new records, if created, contain sufficient information to allow for a continuity of care. At present the GP would initiate any change of NHS number or identity if it was considered appropriate to do so, following the adoption.

The Trust has produced separate guidance on the Adoption Process and the recording of an adopted child’s clinical information in any new record created after their adoption. The guidance also covers clinical record keeping requirements as the child progresses through the adoption process. Any healthcare professional involved in the care and treatment of a child going through the adoption process should ensure they are aware of the latest guidance and contact the Community Paediatrics Adoption Team for further guidance.

14.2 Health Records of Transgender Persons
A patient can request that their gender be changed in a record by a statutory declaration, but this does not give them the same rights as those that can be

---

made by the Gender Recognition Act 200467. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. At this time a new NHS number can be issued and a new record can be created, if it is the wish of the patient. It is important to discuss with the patient what records are moved into the new record and to discuss how to link any records held in any other institutions with the new record.

14.3 Witness Protection Health Records
Where a record is that of someone known to be under a witness protection scheme, the record must be subject to greater security and confidentiality. It may become apparent (such as via accidental disclosure) that the records are those of a person under the protection of the Courts for the purposes of identity. The right to anonymity extends to medical records. For people under certain types of witness protection, the patient will be given a new name and NHS Number, so the records may appear to be that of a different person.

14.4 Use of the NHS Number in HM Prisons
The Health and Justice Information System promotes the use of NHS Numbers within HM Prisons with the aim of ensuring that when a patient has an NHS Number it is included in their patient record4.

The current Prison clinical system (TPP SystmOne) provides functionality for users to enter a prisoner's NHS number if it is available from healthcare records received from other NHS organisations. However, the NHS Number is not a required field to set up a patient record on TPP SystmOne Prison and the use of the NHS number in prisons is not yet mandatory.

It is acknowledged that it is good practice for the NHS Number to be added to the patient record in the clinical IT system where it is available and furthermore to ensure that it is clearly stated on any communication with other NHS organisations when appropriate. It is possible that a patient in prison will not have an NHS Number or does not know it. Furthermore it may be difficult to trace an NHS Number if they are not registered with GP, have no fixed abode or are foreign nationals. If the NHS Number is not available and cannot be traced, this should not delay making a necessary referral to another healthcare organisation.

15 Access to Records
Each Service or department that holds its own clinical records is responsible for ensuring only those members of staff who need to access the records can do so. For electronic clinical systems this should be covered by the use of user access controls/settings with the appropriate access to areas of the system relevant for their roles e.g. use of Smartcards. In order to direct any requests to access records from patients, other services, departments or relevant agencies, members of staff should be aware of who their Local Records Management Lead is. Where no Local Records Management Lead has been identified the Local Team Leader will be take on this responsibility.

---

4 https://digital.nhs.uk/article/283/Health-and-Justice-Information-Services
15.1 **Subject Access Requests**

Under the Data Protection act a patient/client has the right to see their clinical records. They must submit a request in writing (a Subject Access Request), upon receipt of which they will normally be given access to everything recorded about them. This information may not include confidential information about a third party, or information that a healthcare professional considers likely to cause serious harm to the physical or mental health of the patient or someone else.

A patient/client can also ask for access to be given to other people e.g. a solicitor. A Subject Access Request must be submitted detailing the information required and the signed consent of the patient/client. These requests must be sent to the appropriate Service/Department’s Data Protection Liaison Officer (DPLO). For a list of these Data Protection Liaison Officers and further details refer to the Trust’s Data Protection Policy. If you are unable to identify the local Data Protection Liaison Officer the Service Lead for that Service or Department should be contacted and they can advise. The Trust’s Data Protection Officer is the Information Governance Manager.

15.2 **Access to Deceased Patient Records**

If the request is for a deceased patient this comes under the Access to Health Records Act (1990) which allows access to a deceased patient’s records in limited circumstances. It allows access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased’s estate. It should be noted that this is subject to certain restrictions e.g. if the patient has left a note to say access should not be given if an application is made after their death. Any requests for access to deceased patient’s records would be covered by the same principles as for a Subject Access Request.

For further guidance contact the Trust’s Caldicott Guardian, Information Governance / Data Protection Lead or Records Manager.

15.3 **Access to Inpatient Services Medical Records Outside Normal Working Hours**

For the Trust’s inpatient services, Medical Records are obtained from the appropriate services records staff during normal office hours.

Outside these times, the following arrangement apply to Community Hospitals:

- Records can be accessed by the Senior Nurse on duty, either from a location on the site or by transfer from the Acute Hospitals.

16 **Tracking**

A tracking system for all paper records must be in place to ensure that all information can be found quickly and easily. This can be either manual e.g. register book, an index card system or electronic e.g. a spreadsheet or database. A combination of the two could be used to ensure anyone looking for the record is aware where to find it.

The recommended system is the use of a tracer card (see example Appendix 3) that is kept in the record when filed away but is then left in place of the record in the filing system recording its whereabouts. Anyone looking for the original record will find the tracer card and be able to trace it. Backing this up by recording the
information on an electronic system (ideally on a shared network resource) means that a member of staff can check the electronic system first. This will also give central means of tracking and following up records that need retrieving or are overdue for return.

To ensure that information is correct all departments/services must ensure that their tracking processes are documented and these systems are routinely checked and updated.

Tracking systems must record the following (minimum) information:

- The reference number of the record – the use of the NHS number is recommended but this can be the NHS Number and a local reference number
- Person (must be a named individual), role, unit, department and contact number of where the record has been sent
- Brief reason for transfer
- Date of transfer
- Date due back
- Date record was received back

**17 Retrieval of Paper Records**

It is important that all clinical paper records can be retrieved when required. The relevant tracking systems detailed above will support this requirement. Local processes must be documented and in place in order to ensure that anyone accessing clinical paper records is aware of their responsibilities including information security, quality and confidentiality. The Local Records Management Leads or the Local Team/Service Leader for the particular service should be contacted if a paper record retrieval is required from that service. The Trust’s Records Manager can give further advice and guidance if required.

The NHS Number must be used in the process of retrieving paper records and verifying that the records are the correct ones.

**18 Movement of Paper Records**

Security and confidentiality of records must be paramount. In order to ensure access to paper records by authorised members of staff, there is a need to move or transport records either by hand or by post. It is important that both the security and the physical protection of the records are considered.

**18.1 Taking Paper Records off site**

Records must never be taken off site unnecessarily or without the approval of the line manager. When transporting paper records the following advice must be followed:

- All records must be tracked to ensure their location is known
- Records must be carried in sealed envelopes, document/secure mail pouches or suitable secure containers
- Records must be handled carefully into vehicles to ensure they are not damaged by the movement of the vehicle
18.2 Labelling and Packaging of Records for Transporting

When records are being delivered to another location they must be:

- Tracked to ensure their location is known
- Sealed in envelopes or secure mail pouches / wallets
- Packages must be correctly addressed to a named individual detailing their role, service/department and location
- Packages containing personal information must be marked “Private and Confidential”
- Large quantities of records must be transported in suitable, secure boxes or containers for their protection

It is the sender’s responsibility to ensure the records are sent to the correct location by a secure means whether this is internal transport or a courier.

It is good practice to e-mail the recipient to notify them that the records are being sent and to ask for a confirmation e-mail when they have arrived. This ensures that records are transferred in a timely manner and any non-delivery can be followed up promptly.

Please refer to the Trust’s Information Security Policy for up to date guidance.

18.3 Electronic Records

Particular attention must be taken concerning security and confidentiality of electronic records when transmitting electronically or transferring to other media e.g. a memory stick. It is the sender’s responsibility to ensure the information is transmitted securely e.g. encrypted/send secure.

Detailed guidance on this can be found in the Trust’s Information Security Policy and the Information Governance Policy, Confidentiality section.

19 Storage of Paper Records

Paper records must always be kept securely and contained in a locked room or locked cabinet within a secure location. A sensible balance must be achieved between the need for security and accessibility. Records must not be left in a position where an unauthorised person can obtain access to them, whether they are hard copy or electronic. They must not be left unattended at any time unless they are in a secure lockable area. The clinical records must be stored in the approved records storage area for that service. Clinical records can be tracked out for a period of time to a location where the patient is most often seen or where the service responsible for the care is based but the records must be returned to the approved storage area when the record is no longer active. Each service is required to store records in an environment that does not cause damage or decay to the documentation within the record.

Secure off-site storage is available for less frequently used/inactive records. See the retention and disposal section below for further information.

For more detailed guidance on security of information see the Trust’s Information Security Policy.
20 Mobile and Homworking

It is recognised that there is a need for some staff to work from other locations including at home. There are specific requirements and guidelines relating to this in particular the Mobile and Home Working Overview in the Information Security Policy. Staff undertaking this type of work must refer to that guidance and the relevant sections detailed in this policy but in summary the key points are:

- Staff must have permission from their line managers to undertake mobile or homeworking and be aware of their responsibilities
- Ensure appropriate security measures are identified and followed for both electronic and hard copy records. This includes encryption of electronic data and logging out when you are not using the computer
- The use of secure containers for paper records in transit and at locations e.g. lockable briefcase, secure mail pouch or filing cabinet
- Confidentiality: records must not be accessible to unauthorised persons e.g. family or friends at home or by other commuters whilst travelling
- Tracking: records must be able to be traced if required by others
- Data on Laptops must be regularly backed up and archived when no longer required

Remember it is the individual’s responsibility to safeguard the information they are using.

21 Retention and Disposal

The Trust’s Records Management Policy, Records Retention section gives full details on the Trust’s records retention and disposal processes (for both Clinical and Corporate records) and should be referred to for advice and guidance on this topic.

The basic concept is that when records are no longer required for operational purposes they can be sent to a secure off site location for archiving. It is important that any records archived must be able to be retrieved at a later date if required or disposed of when they come to the end of their retention period. A Records Retention and Archiving register must be kept by each service / department.

All clinical records are confidential so, when required, they must be destroyed using a confidential destruction method (e.g. crosscut shredding for hard copy records) but it is recommended that a Confidential Waste and Recycling Service is used. Not only is this environmentally friendly it also provides proof of safe destruction i.e. Certificates of Destruction. For further advice and guidance on these services contact the Records Manager.

22 Records Audit

The auditing of records and acting on the results is a good means of assuring the quality of clinical record keeping, the clinical record keeping systems and administration processes and will identify any areas where improvements can be made. A key finding of the Francis Report was the need to carry out regular clinical record keeping audits. These audits will also assist services in managing the risks associated with the quality of clinical records. It is also a good means of identifying and sharing good practices.
22.1 Clinical Record Keeping Audit

It is recommended that clinical record keeping audits are carried out on an annual basis. This will ensure there is an ongoing audit cycle. If this is not practical then, as a minimum, these audits must be carried out every three years.

The Clinical Record Keeping Audit planning process (Appendix 5) gives an overview of the recommended approach to planning a clinical record keeping audit. The Clinical Record Keeping Audit Form Template (Appendix 6) has been designed as a basis for all audits. Audit samples will be defined based on a percentage of the caseloads, the number of service/clinic locations and the number of healthcare professional working within that particular service. To assist in the efficiency of carrying out these audits and collating the resulting data an online Audit and Survey Tool is available and can be set up for individual audits.

The Clinical Audit Team and Records Manager are available to give further specific advice, support and guidance in planning and undertaking audits.

23 Consultation

This policy has been developed by the Records Manager in consultation with representatives from services across the organisation through the Records Management Group and relevant local team meetings and discussions. The Records Manager has also discussed particular areas with relevant specialist staff and clinical leads. The policy has also been presented to the Information Governance Operational Group for final ratification.

24 Dissemination

This policy will be disseminated by the following methods:

- Published on the Trust website
- Directors to disseminate to managers and staff within their areas
- A Trust newsletter article
- The Records Manager supported by the Local Records Management Leads and Service Managers will raise the awareness of the clinical record management standards, best practices and guidance.
- The Information Governance training will cover relevant aspects of these standards.
- Awareness raising by managers and team leaders at local inductions and team meetings

25 Advice

The following are available to give advice relating to topics covered in this policy:

Records Manager and Quality Facilitator

Alan Ferguson
Tel: 01743 277617, E-mail: alan.ferguson@nhs.net
Caldicott Guardian
Steve Gregory, Director of Nursing and Operations
Tel: 01743 277588, E-mail: steve.gregory@nhs.net

Information Governance Manager (Information Governance and Data Protection Officer)
Gill Richards
Tel: 01743 871998, E-mail: gill.richards8@nhs.net

Further guidance is available on the Records Management page of the website:
www.shropscommunityhealth.nhs.uk/recordsmanagement

26 Training
Records Management is part of Information Governance and the training available is detailed in the Trust’s Mandatory (Risk Management) Training Policy and Procedure.

For further information contact:
Deborah Hammond - Organisational Development Manager:
E-mail: deborah.hammond@nhs.net

Additional bespoke Record Keeping Training can be arranged through the Records Manager

27 Review
This policy will be reviewed by the Records Manager every two years or earlier if there are changes to legislation or regulations relating to clinical record keeping.

28 Compliance Monitoring
To achieve compliance with the Care Quality Commission and the Information Governance Toolkit requirements regular audits of record keeping standards and practice will be undertaken, co-ordinated by the Records Manager.

29 Related Documents
Trust policies, procedures and other records management related documents:

- Records Management Policy (incorporating the Records Retention, Archiving and Disposal process)
- Information Governance Policy (incorporating Confidentiality, Data Protection and Freedom of Information)
- Mandatory Training Policy
- Information Security Policy
- Information Quality Assurance Policy
- Consent to Examination and Treatment Policy
- Patient and Public Information Policy
- Clinical Photography Guidelines
- “Your Information: what you need to know” leaflet

These documents are available on the Trust’s website:
http://www.shropscommunityhealth.nhs.uk/policies
30 References

- Care Quality Commission: Fundamental standards - Good Governance (Regulation 17) http://www.cqc.org.uk/content/fundamental-standards
- Information Governance Toolkit requirements: https://www.igt.hscic.gov.uk/
- Nursing and Midwifery Council (NMC) The Code https://www.nmc.org.uk/standards/code/
- Health and Social Care Professions Council (HCPC) Standards http://www.hpc-uk.org/publications/standards/
- Relevant Professional Codes of Practice for Allied Healthcare Professionals
- Access to Health Records Act 1990
- Data Protection Act 2018
- Human Rights Act 1998
- Public Records Act 1958
- Mental Capacity Act 2005
- The Summary Care Record: http://systems.hscic.gov.uk/scr

31 Glossary

31.1 Definitions

<table>
<thead>
<tr>
<th>Word</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive</td>
<td>Those records that are appraised as having permanent value.</td>
<td>National Archives</td>
</tr>
<tr>
<td>Disposal</td>
<td>The implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement</td>
<td>National Archives</td>
</tr>
<tr>
<td>Word</td>
<td>Definition</td>
<td>Source</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Encryption</td>
<td>Encryption is the means of converting information using a code that prevents it being understood by anyone who isn't authorised to read it. Files, emails, even whole hard drives can be encrypted. As a general rule the more bits used for encryption the stronger it will be, so 128-bit is stronger than 64-bit.</td>
<td>Get Safe Online Organisation</td>
</tr>
<tr>
<td>Jointly Held Records</td>
<td>A record held jointly by health and social care professionals, for example in a Mental Health and Social Care Trust. A jointly held record should be retained for the longest period for that type of record, i.e. if social care has a longer retention period than health, the record should be held for the longer period.</td>
<td>NHS Code of Practice</td>
</tr>
<tr>
<td>Master Patient Index (MPI)</td>
<td>In medical systems the Master Patient Index (MPI) is an index referencing all patients known to an area, enterprise or organisation. The terms Patient Master Index (PMI) and Master Patient Index are used interchangeably.</td>
<td>NHS Code of Practice</td>
</tr>
<tr>
<td>NHS Care Records Service</td>
<td>The NHS Care Records Service (NHS CRS) will connect all GPs, acute, community and mental health NHS trusts in a single, secure national system that will enable individual electronic patient record details to be accessed by authorised personnel, at the appropriate level, anywhere in England, via use of a unique identifier. The unique identifier to be employed throughout the NHS and its associated systems is the NHS number.</td>
<td>NHS Code of Practice</td>
</tr>
<tr>
<td>NHS Number</td>
<td>Introduced in 1996, the NHS number is a unique 10 character number assigned to every individual registered with the NHS in England (and Wales). The first nine characters are the identifier and the tenth is a check digit used to confirm the number's validity. Babies born in England and Wales are allocated an NHS number by Maternity Units, at the point of Statutory Birth Notification. The NHS number is used as the common identifier for patients across different NHS organisations and is a key component in the implementation of the NHS CRS.</td>
<td>NHS Code of Practice</td>
</tr>
<tr>
<td>NHS Record</td>
<td>An NHS record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees - including consultants, agency or casual staff.</td>
<td>NHS Code of Practice</td>
</tr>
</tbody>
</table>
### Personal Confidential Data (PID)

Personal Confidential Data is data that contains sufficient information to be able to identify the specific person to whom the data belongs (patient or staff) e.g. name, date of birth, address. This generally excludes publicly available contact lists e.g. staff telephone directories. Also previously referred to as Personal Identifiable Data (PID).

### Record

Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business. (BS ISO 15489.1)

### Register

A list of records, usually in simple sequence such as date and reference number, serving as a finding aid to the records.

### Retention

The continued storage and maintenance of records for as long as they are required by the creating or holding organisation until their eventual disposal, according to their administrative, legal, financial and historical evaluation.

### Tracking

Creating, capturing and maintaining information about the movement and use of records. (BS ISO 15489-1:2001)

### Transfer of Records

Transfer (custody) - Change of custody, ownership and/or responsibility for records. (BS ISO 15489-1:2001) Transfer (movement) - Moving records from one location to another. (BS ISO 15489-1:2001) Records identified as more appropriately held as archives should be offered to The National Archives, which will make a decision regarding their long-term preservation.

### 31.2 Abbreviations

<table>
<thead>
<tr>
<th>Term / Abbreviation</th>
<th>Definition / description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AHP</td>
<td>Allied Health Professional</td>
</tr>
<tr>
<td>CQC</td>
<td>Care Quality Commission</td>
</tr>
<tr>
<td>DH</td>
<td>Department of Health</td>
</tr>
<tr>
<td>DfE</td>
<td>Department for Education</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>EPR</td>
<td>Electronic Patient Record</td>
</tr>
<tr>
<td>Term / Abbreviation</td>
<td>Definition / description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>FOI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>GMC</td>
<td>General Medical Council</td>
</tr>
<tr>
<td>HPC</td>
<td>Health Professions Council</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office</td>
</tr>
<tr>
<td>IG</td>
<td>Information Governance</td>
</tr>
<tr>
<td>IGT</td>
<td>Information Governance Toolkit</td>
</tr>
<tr>
<td>IM&amp;T</td>
<td>Information Management and Technology</td>
</tr>
<tr>
<td>MCA</td>
<td>Mental Capacity Act</td>
</tr>
<tr>
<td>MPI</td>
<td>Master Patient Index</td>
</tr>
<tr>
<td>NHS CRS</td>
<td>NHS Care Records Service</td>
</tr>
<tr>
<td>NHSLA</td>
<td>NHS Litigation Authority</td>
</tr>
<tr>
<td>NMC</td>
<td>Nursing and Midwifery Council</td>
</tr>
<tr>
<td>PALS</td>
<td>Patient Advice and Liaison Service</td>
</tr>
<tr>
<td>PCD</td>
<td>Personal Confidential Data</td>
</tr>
<tr>
<td></td>
<td>Note: previously Personal Identifiable Data (PID)</td>
</tr>
<tr>
<td>SCHT</td>
<td>Shropshire Community Health NHS Trust</td>
</tr>
</tbody>
</table>
Appendix 1: Record Keeping Related Legislation, National Standards and Requirements

Records Management Code of Practice for Health and Social Care 2016
The Records Management Code of Practice for Health and Social Care 2016 has been published by the Information Governance Alliance (IGA) for the Department of Health (DH).

This Records Management Code of Practice for Health and Social Care 2016 (from this point onwards referred to as the Code) is a guide for you to use in relation to the practice of managing records. This Code is relevant to organisations who work within, or under contract to NHS organisations in England. This also includes public health functions in Local Authorities and Adult Social Care where there is joint care provided within the NHS.

The Code is based on current legal requirements and professional best practice. It will help organisations to implement the recommendations of the Mid Staffordshire NHS Foundation Trust Public Inquiry relating to records management and transparency.

The Code was drafted by a working group of representatives from the Information Governance Alliance, the Health and Social Care Information Centre, NHS England, the Department of Health, The National Archives and from a range of NHS and social care organisations, including Acute and integrated Mental Health Trusts, Clinical Commissioning Groups, GP practices and professional bodies.

The Code is a key component of information governance arrangements for the NHS. Standards and practice covered by the Code will change over time so this document will be reviewed regularly and updated as necessary.

This Code of Practice replaces the previous guidance listed below:

- HSC 1999/053 – For the Record
- HSC 1998/217 – Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients (Replacement for FHSL (94)(30))


The Data Protection Act 2018
Keeping records is the responsibility of all Trust staff. Staff must consider and understand the following guidance on the Data Protection Act and seek advice from the Information Governance Lead.

The Data Protection Act Principles:
Everyone responsible for using personal data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

a) used fairly, lawfully and transparently
b) used for specified, explicit purposes

c) used in a way that is adequate, relevant and limited to only what is necessary

d) accurate and, where necessary, kept up to date

e) kept for no longer than is necessary

f) handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

Subject Access Request

Under the above data protection legislation individuals have a right to make requests to the Trust regarding the use of their information; this is called a Subject Access Request (SAR). The Trust, as a Data Controller, must respond to these requests “without undue delay and at the latest within one month of receipt”.

In most cases the Trust does not make a charge for Subject Access Requests. A reasonable fee may be made in exceptional circumstances

General Data Protection Regulation (GDPR)

The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, replaced the Data Protection Directive 95/46/ec in Spring 2018 as the primary law regulating how companies protect EU citizens' personal data. It is regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.


DPA / GDPR terms:

- “data subject” means an individual who is the subject of personal data;
• “personal data” means any information relating to an identified or identifiable natural person

• “relevant filing system” means any structured set of personal data which are accessible according to specific criteria, whether centralised, de-centralised or dispersed on a functional or geographical basis. The Data Protection Act defines this as:

> “any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.”

• “third party” means information that relates to and identifies a third party individual.

• “health professionals” includes Occupational Health Advisors

• “personnel file” may include the Occupational Health file

**Access to Health Records Act 1990**

The Access to Health Records Act (AHRA) 1990 provides certain individuals with a right of access to the health records of a deceased individual. These individuals are defined under Section 3(1)(f) of that Act as, ‘the patient’s personal representative and any person who may have a claim arising out of the patient’s death’. A personal representative is the executor or administrator of the deceased person’s estate.

The personal representative is the only person who has an unqualified right of access to a deceased patient’s record and need give no reason for applying for access to a record. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient’s death. Record holders must satisfy themselves as to the identity of applicants who should provide as much information to identify themselves as possible. Where an application is being made on the basis of a claim arising from the deceased’s death, applicants must provide evidence to support their claim. Personal representatives will also need to provide evidence of identity.

**Applying for Access to Records under AHRA**

A request for access should be made in writing to the record holder ensuring that it contains sufficient information to enable the correct records to be identified. Applicants may wish to specify particular dates or parts of records which they wish to access. The request should also give details of the applicant’s right to access the records.

Once the data controller has the relevant information, they should comply with the request promptly and within 21 days where the record has been added to in the last 40 days, and within 40 days otherwise. In most cases the Trust does not make a charge for requests under the Access to Health Records Act. A reasonable fee may be made in exceptional circumstances.

**Care Quality Commission – Fundamental Standards**

As the regulator of health and adult social care in England, the Care Quality commission (CQC) make sure that the care that people receive meets essential
standards of quality and safety and they encourage ongoing improvements by those who provide or commission care. The fundamental standards are the standards by which the CQC stipulate that a care service provider must never fall below. Everybody has the right to expect care within these standards and they form part of the law.

**Regulation 17: Good Governance (records management extract)**

17(2)(c) maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided;

17(2)(d) maintain securely such other records as are necessary to be kept in relation to:

(i) persons employed in the carrying on of the regulated activity, and

(ii) the management of the regulated activity;

CQC Website - Regulation 17 link: [http://www.cqc.org.uk/content/regulation-17-good-governance](http://www.cqc.org.uk/content/regulation-17-good-governance)

**Data Security and Protection Toolkit (DSPT)**

The Data Security and Protection Toolkit (DSPT) replaces the Information Governance Toolkit (IG Toolkit). It forms part of a new framework for assuring that organisations are implementing the National Data Guardian’s 10 data security standards and meeting their statutory obligations on data protection and data security. The DSPT is an online self-assessment tool that allows organisations to measure their performance against these 10 standards

1. **Data Security Standard 1.** All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

2. **Data Security Standard 2.** All staff understand their responsibilities under the National Data Guardian’s Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

3. **Data Security Standard 3.** All staff complete appropriate annual data security training and pass a mandatory test, provided through the Data Security and Protection Toolkit.

4. **Data Security Standard 4.** Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

5. **Data Security Standard 5.** Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

6. **Data Security Standard 6.** Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
7. **Data Security Standard 7.** A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

8. **Data Security Standard 8.** No unsupported operating systems, software or internet browsers are used within the IT estate.

9. **Data Security Standard 9.** A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

10. **Data Security Standard 10.** IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian’s Data Security Standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

**Accessible Information Standard 2016**

From 1st August 2016 onwards, all organisations that provide NHS care or adult social care are legally required to follow the Accessible Information Standard.

The standard aims to make sure that people who have a disability, impairment or sensory loss are provided with information that they can easily read or understand and with support so they can communicate effectively with health and social care services.

The Accessible Information Standard says that people who have a disability or sensory loss should get information in a way they can access and understand. To ensure that people using our services receive information in the way they can access and understand there are five basic steps you should follow.

**Five Basic Steps**

1. **Ask:** identify / find out if an individual has any communication / information needs relating to a disability or sensory loss and if so what they are

2. **Record:** record those needs in a clear, unambiguous and standardised way in electronic and / or paper based record / administrative systems / documents

3. **Alert/Flag/Highlight:** ensure that recorded needs are ‘highly visible’ whenever the individual’s record is accessed, and prompt for action.

4. **Share:** include information about individuals’ information / communication needs as part of existing data sharing processes (and in line with existing information governance frameworks).

5. **Act:** take steps to ensure that individuals receive information which they can access and understand, and receive communication support if they need it.

NHS England AIS website: [https://www.england.nhs.uk/ourwork/accessibleinfo/](https://www.england.nhs.uk/ourwork/accessibleinfo/)
Appendix 2: Example Records Register
The following table gives an outline of the suggested headings to be used in a Records Register. This will enable the register to be used to both record the active records but also keep a trace on records movements:

<table>
<thead>
<tr>
<th>Date of Record</th>
<th>First Name</th>
<th>Last Name</th>
<th>DoB (dd/mm/yyyy)</th>
<th>NHS Number (nnn nnn nnnn)</th>
<th>Healthcare Professional</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Record Out (dd/mm/yyyy)</th>
<th>Name of Person Receiving Record</th>
<th>Service/Location</th>
<th>Due Back (dd/mm/yyyy)</th>
<th>Records In (dd/mm/yyyy)</th>
<th>Comments</th>
<th>Record Closed (dd/mm/yyyy)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix 3: Example Tracer Card

**Tracer Card**

<table>
<thead>
<tr>
<th>Date Out:</th>
<th>Issued to: (incl. contact details)</th>
<th>Reason:</th>
<th>Issued by (initials):</th>
<th>Date Due Back:</th>
<th>Date Returned:</th>
<th>Returned to (initials):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix 4: Example Clinical Document Format and Layout

```
First Name: __________________________
Last Name: __________________________
Date of Birth: ________________________
NHS No: _____________________________

Date & Time  |  Signature, Print Name & Designation

Footer
<<Doc Ref and Version>>  <<Page No>>  <<Month and year>>
```
Appendix 5: Clinical Record Keeping Audit planning

The following guidance on audit planning is available as a separate document. Anyone undertaking a Record Keeping Audit should contact the Records Manager for the most up to date version.

Introduction

Maintaining high standards of record keeping is the duty of all health professionals and clinical audit is the method of assuring that this is taking place. Clinical record keeping audits need not be complex and in order to help you with the process a record keeping audit template form and supporting documentation have been produced.

Planning

As part of the Trust’s Clinical Audit Programme the Clinical Audit Team should be notified of any clinical record keeping audits that Services want to carry out. Service Managers will nominate a lead person who will be responsible for setting up the audit, feeding back the results and, in conjunction with the service manager, reviewing training needs and implementing any changes identified.

The involvement of the Clinical Audit Team, the Records Manager and clinical and administrative representatives from the particular service is important to ensure that everyone understands all aspects of the audit and the particular record keeping processes of the service involved. Having sample records at hand at an initial meeting is useful in order to ensure the audit questions are relevant and that any additional questions can be identified.

Other areas to be covered in the planning stage include:

- Completion of an audit proposal
- Who will carry out the audit?
- Frequency of the audit process
- Development of an appropriate Clinical Record Keeping Audit Form
- Understanding of the audit reporting requirements and process

In general terms the record keeping audits consist of:

Aim of the audit: To ensure compliance with the relevant national, regional, professional and local clinical record keeping requirements

Objectives:

- To give evidence based assurance that clinical record keeping standards and best practice is being carried out within the service
- To ensure a consistent approach to clinical record keeping practices
- To identify any areas of concern within the clinical record keeping practices
- To highlight areas of good practice that can be shared with other services
- To identify gaps or areas for future training
- To develop action plans to resolve any concerns or issues identified
Audit Proposal
Every audit carried out requires the completion of an Audit Proposal form which is available from the Clinical Audit Team and should be returned to them so that it is logged within the audit programme.

Who carries out the Audit?
Depending on the aim of the audit it could be carried out by:

1. **The Audit Lead** – this might be from a managerial aspect or in order to gain a better insight into their particular service.

2. **Fellow Professional / Peer reviewer** – good for when the professional content of the records is being reviewed e.g. clear description of problem given, assessment recorded and evaluation. The advantage of this method is that best practice is then shared.

3. **Designated professional or administrative staff** – this may be where additional support is required to enable the service to carry out the audit.

Prior training may need to be undertaken in order to ensure that a consistent approach is being taken when undertaking the audit.

Records Sample
Sufficient records must be audited to obtain an accurate representation of the overall standard of record keeping across the service. This must take into account the staff completing the records and the locations they are based at or cover. Records must be chosen at random. The initial audit sample may be small but if the audit analysis highlights any issues a larger sample can be used on a follow up audit.

Frequency of the audit process
It is recommended that clinical record keeping audits are carried out annually but each service or professional group must audit its record keeping standards at least once every three years. Service Managers / Team Leads must undertake a risk assessment to determine if audits should take place more frequently.

With the introduction of the Electronic Patient Record system (RiO), which gives easier access to the patient records, services are expected to carry out a record keeping audit every year.

Frequency of audit will also be determined by the outcome of a previous audit. Where poor record keeping standards are found, then training and further audit should take place within 6 months. Audits should always be considered as part of an Audit Lifecycle and not a one off process.

Clinical Record Keeping Audit Form
The Clinical Record Keeping Audit form template is to be considered a starting point for any clinical record keeping audits. It gives a good selection of questions which are designed to cover all areas that need to be considered and are based on best practice guidance contained within relevant NHS, professional and organisational codes of practice and standards.
The audit tool is split into the following sections:

**Section A: Patient Demographics:** to ensure all the patient details are up to date and correct

**Section B: Does the record provide clear evidence of:** This is the section to ensure we have the evidence to give assurance that we are delivering the relevant care from referral through to discharge

**Section C: Records Entries** (check progress notes, forms and relevant assessments) in this section we check to ensure the relevant records entries are complete and accurate

**Section D: Scanning and Uploading documents to RiO** (where documents are uploaded to the patient’s record) This section is to ensure that any documents scanned/uploaded are legible can be easily identified and retrieved

**Section E: Paper Records:** (if a paper aspect of the record is maintained as part of the patient’s care and treatment the following section needs to be completed). This section ensures we are maintaining the relevant professional and record keeping standards for any associated paper records

In the planning stage the actual questions required for the specific audit will be discussed and agreed and a specific form designed for that audit. To assist in the efficiency of carrying out these audits and collating the resulting data an online Audit and Survey Tool will be set up for individual audits based on the agreed clinical record keeping audit template. The Records Manager must be contacted for the latest version of the Clinical Record Keeping Audit Form Template (see Appendix 6 for example template). Please ensure the Records Manager is consulted to ensure the latest version of the Audit Tool is being used.

**Reporting Audit Findings**

The lead person for the audit is responsible for completing an Audit Report, and reporting the audit findings back to their professional group or service and to the service manager, and developing an action plan based on the findings. The action plan must describe any changes that need to be made to the records format, any staff training needs and the time frame for re-audit.

**Audit Reports**

Audit reports must be completed for each audit as a record of the whole audit process. The suggested content of these reports is as follows:

- Introduction/Background
- Aim
- Objectives
- Standards
- Criteria
- Methodology
- Findings and Recommendations
- Action Plan
- Appendices: containing tables and charts and example audit forms and other relevant documents used in the audit
The Stages of Clinical Audit:

### Clinical Record Keeping Audit Form

<table>
<thead>
<tr>
<th>Service Deliver Group:</th>
<th>(Adults, Children &amp; Families, TEMS &amp; Outpatients select from drop down list)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service:</td>
<td>(Select from drop down list)</td>
</tr>
<tr>
<td>Locality:</td>
<td>(if required - Select from drop down list)</td>
</tr>
<tr>
<td>Location:</td>
<td>(if required - Select from drop down list)</td>
</tr>
<tr>
<td>Record Audit Ref:</td>
<td>(Patient initials and last four of their NHS Number e.g. AB1234)</td>
</tr>
</tbody>
</table>

**Section A: Patient Demographics**

1. Is the patient’s record synchronised with the National Demographic System (i.e. the Spine)?
   - Yes ☐ No ☐

2. NHS Number
   - Yes ☐ No ☐

3. First name
   - Yes ☐ No ☐

4. Last Name
   - Yes ☐ No ☐

5. Date of Birth
   - Yes ☐ No ☐

6. Patient contact details *(Address, telephone number)*
   - Yes ☐ No ☐

7. Is the patient’s gender recorded?
   - Yes ☐ No ☐

8. Is the patient’s ethnicity recorded?
   - Yes ☐ No ☐

9. Are other relevant contact details recorded in the record *(e.g. Next of Kin, Carers, Lasting Power of Attorney)*?
   - Yes ☐ No ☐

10. For children and young people is Parental Responsibility recorded in the record?
    - Yes ☐ No ☐ n/a ☐

11. Where applicable, are the patient details recorded in the paper record the same as recorded on the Electronic Patient Record system *(e.g. RiO)*? *(Note: this question only relevant in certain services)*
    - Yes ☐ No ☐ n/a ☐

12. Comments for Section A *(continue on additional page if required)*

**Section B: Does the record provide clear evidence of:**

13. Referral / transfer of care information received?
    - Yes ☐ No ☐

14. Relevant Past Medical History?
    - Yes ☐ No ☐
15. Relevant Clinical Indicators/Alerts checked and recorded?  
   Yes ☐  No ☐  n/a ☐

16. Allergies checked and recorded?  
   Yes ☐  No ☐

17. Presenting condition / problem?  
   Yes ☐  No ☐

18. Assessments carried out?  
   Yes ☐  No ☐

19. The decisions made?  
   Yes ☐  No ☐

20. The care planned?  
   Yes ☐  No ☐

21. Do the Progress Note entries contain sufficient information to inform others of the care and treatment provided and signpost them to other relevant information within the record?  
   Yes ☐  No ☐

22. Evidence of care / treatment plan being reviewed at each appointment?  
   Yes ☐  No ☐

23. All required care delivered to date as planned?  
   Yes ☐  No ☐

24. The notes having been written with the involvement of the patient and / or parent / carer e.g. in discussions about assessment / plan / outcome?  
   Yes ☐  No ☐

25. The information / leaflets shared with patient and / or parent / carer?  
   Yes ☐  No ☐  n/a ☐

26. If applicable, appropriate Transfer / Discharge of Care?  
   Yes ☐  No ☐  n/a ☐

27. Comments for Section B (continue on additional page if required)

Section C: Records Entries (check progress notes, forms and relevant assessments)

28. Dated *(to reflect date of contact/intervention)*  
   Yes ☐  No ☐

29. Timed *(to reflect time of contact/intervention)*  
   Yes ☐  No ☐

30. Are there any abbreviations in the last entry?  
   Yes ☐  No ☐

31. If Yes, is the abbreviation written in full at first entry?  
   Yes ☐  No ☐  n/a ☐

32. Or, if Yes, is it an approved abbreviation?  
   Yes ☐  No ☐  n/a ☐

33. If applicable is there a list of approved abbreviations uploaded to the record?  
   Yes ☐  No ☐  n/a ☐

34. Was appropriate consent for care/treatment obtained and recorded  
   Yes ☐  No ☐

35. Is there a record of an existing paper record and where it is stored?  
   Yes ☐  No ☐  n/a ☐

36. Additional communication/accessibility needs – identified and recorded (as per the Accessible Information Standard requirements)?  
   Yes ☐  No ☐  n/a ☐

37. Relevant protected characteristics information recorded e.g. Learning Disabilities?  
   Yes ☐  No ☐  n/a ☐

38. Is the need for a Mental Capacity Act Assessment recorded? *(Note: not applicable to under 16s)*  
   Yes ☐  No ☐  n/a ☐

39. If applicable, has the child/young person’s competence been assessed and recorded in line with Fraser Guidelines?  
   Yes ☐  No ☐  n/a ☐
40. Are there any subjective or offensive statements?  Yes ☐ No ☐

41. Are all relevant forms completed fully?  (If not please give details in the Comments section below)  Yes ☐ No ☐

42. Are the record entries validated?  Yes ☐ No ☐

43. Was there a record made of other people present during the consultation (e.g. chaperone, carer, other healthcare professional)?  Yes ☐ No ☐ n/a ☐

44. Are the notes written in terms that a patient and/or parent/carer can understand?  Yes ☐ No ☐

45. Are the notes written in terms that another professional involved in the care of the patient can understand?  Yes ☐ No ☐

46. Does the patient have an appropriate “Referral to Treatment” (RTT) pathway recorded?  Yes ☐ No ☐ n/a ☐

47. Are medications accurately and appropriately recorded?  Yes ☐ No ☐ n/a ☐

48. Is the patient’s care and treatment still appropriate for this Service?  Yes ☐ No ☐

49. Do all appointments have activity recorded?  Yes ☐ No ☐

50. Are all appointments outcomed?  Yes ☐ No ☐ n/a ☐

51. Comments for Section C (continue on additional page if required)

---

**Section D: Scanning and Uploading documents to RiO**

52. Are there any uploaded documents in the patient record?  Yes ☐ No ☐

*Note: if Yes continue in this section if no continue to next section*

53. Do the uploaded documents relate to the correct patient?  Yes ☐ No ☐

54. Does the document date field in RiO match the actual date of the document?  Yes ☐ No ☐

55. Can the uploaded documents be found and retrieved by those who need to refer to them i.e. consistent document naming conventions used?  Yes ☐ No ☐

56. Can all the scanned documents be opened?  Yes ☐ No ☐

57. Are the scanned documents legible?  Yes ☐ No ☐

58. Are the scanned documents correctly oriented?  Yes ☐ No ☐

59. Are the pages in the documents scanned in sequential order?  Yes ☐ No ☐

60. Are all required documents stored in the patient’s record?  Yes ☐ No ☐

61. Is the NHS Number included in all clinical correspondence relating to the patient sent out by the Service?  Yes ☐ No ☐
### Section E: Paper Records:

*(if a paper aspect of the record is maintained as part of the patient’s care and treatment the following section needs to be completed)*

63. Is there a paper record maintained as part of the patient’s care and treatment?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

**Note:** If Yes complete this section, if no proceed to end of audit

64. Are the patient’s details recorded? including First Name, Last Name, Date of Birth, NHS Number  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

65. Are their contact details for the Service/Team recorded at the front of the record?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
<th>n/a □</th>
</tr>
</thead>
</table>

66. Is the patient folder in a good state of repair and are all papers filed securely in the notes? (i.e. nothing loose)  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

**Note:** If there are loose items please list in comments section below

67. Is the patient's Name and NHS Number on every page?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

68. Are the record contents in chronological order?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

69. Are continuation sheets numbered consecutively?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

70. Are the entries in the record written clearly?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

71. Are the entries made in permanent ink and readable if photocopied?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

72. Are all relevant forms completed fully?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

73. Are the record entries signed *(identifiable signature)*, printed, dated and timed by the Healthcare Professional?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
<th>n/a □</th>
</tr>
</thead>
</table>

74. Is there a Signature List in the record completed by those delivering care to the patient?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
<th>n/a □</th>
</tr>
</thead>
</table>

75. If applicable is there a list of approved abbreviations in the paper record?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
<th>n/a □</th>
</tr>
</thead>
</table>

76. Are all student entries counter signed by a qualified/supervising staff  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
<th>n/a □</th>
</tr>
</thead>
</table>

77. Are any alterations readable, dated, timed and signed?  

<table>
<thead>
<tr>
<th></th>
<th>No alterations □</th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

78. Has any correction fluid been used to make alterations?  

<table>
<thead>
<tr>
<th></th>
<th>No alterations □</th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

79. Are there any abbreviations in the last entry?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

80. If Yes, is the abbreviation from a list of approved abbreviations or written fully at first entry?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
<th>n/a □</th>
</tr>
</thead>
</table>

81. Do the notes provide evidence of the care and treatment delivered?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

82. Are the notes written in terms that a patient and/or carer can understand?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>

83. Are the notes written in terms that a professional involved in the care of the patient can understand?  

<table>
<thead>
<tr>
<th></th>
<th>Yes □</th>
<th>No □</th>
</tr>
</thead>
</table>
84. Comments for Section E *(continue on additional page if required)*

<table>
<thead>
<tr>
<th>Data collector (1)</th>
<th>Data collector (2) if applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: ______________________________</td>
<td>Name: __________________________</td>
</tr>
<tr>
<td>Job title/role: ____________________</td>
<td>Job title/role: __________________</td>
</tr>
<tr>
<td>Team: ______________________________</td>
<td>Team: __________________________</td>
</tr>
<tr>
<td>Tel No: ____________________________</td>
<td>Tel No: __________________________</td>
</tr>
<tr>
<td>Email: ____________________________</td>
<td>Email: __________________________</td>
</tr>
<tr>
<td>Date completed: ...... / ....... / .......</td>
<td></td>
</tr>
</tbody>
</table>