Policies, Procedures, Guidelines and Protocols

Document Details	
Title	**Records Management Policy**
Trust Ref No	1348/17311
Local Ref (optional)	N/A
Main points the document covers	The policy sets out the arrangements to achieve good records management practice, in line with DH guidance and requirements
Who is the document aimed at?	All staff
Author	Alan Ferguson, Records Manager & Quality Facilitator
Approval process	
Approved by (Committee/Director)	Information Governance Committee
Approval Date	15 May 2012
Initial Equality Impact Screening	Yes
Full Equality Impact Assessment	No
Lead Director	Maggie Bayley, Director of Nursing, Allied Health Professionals, Quality and Workforce
Category	General
Sub Category	Information Governance
Review date	14 May 2014
Distribution	
Who the policy will be distributed to	All staff
Method	Publication on the Trust Website, distribution to Directors and Service Managers for dissemination to staff, Awareness Raising by the Records Manager and Local Records Management Leads.
Document Links	
Required by CQC	Yes
Required by NHLSA	Yes
Other	Information Governance Toolkit

Amendments History		
No	Date	Amendment
1	May 2012	Policy reviewed and updated to reflect changes within the Trust's organisational structure and latest guidance and standards
2		
3		

Contents

1 Introduction

Shropshire Community Health NHS Trust (SCHT) recognises the importance of sound records management arrangements for both clinical and corporate records produced in support of the Trust's purpose to improve the health and well being of our communities, by working with the NHS and allied agencies to deliver high quality services appropriate to the changing needs of the population.

The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

The Trust Board has adopted this Records Management Policy and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits that include:

- Better use of physical and IT network/server space;
- Better use of staff time;
- Improved control of valuable information resources;
- Compliance with legislation and regulatory standards; and
- Reduced costs.

This document was written in accordance with the Department of Health guidance 'Records Management: NHS Code of Practice' (Parts 1 and 2) and explains the Trust's processes for ensuring that all records are:

- Properly controlled,
- Readily accessible, and eventually
- Archived or otherwise disposed of.

It was drawn up with an awareness of the importance to the Trust of good record keeping and to achieve compliance with the following legislation and regulatory requirements:

- The Data Protection Act 1998 (DPA);
- The Freedom of Information Act 2000 (FOI);
- The Access to Health Records Act 1990;
- The Public Records Act 1958 and 1967;
- Mental Capacity Act 2005;
- Care Quality Commission (CQC) – Essential standards for quality and safety;
- NHS Connecting for Health (NHS CFH) Information Governance Toolkit (IGT);
- NHS Litigation Authority (NHSLA) Risk Management Standards

See Appendix 1 for a brief summary of the items listed above.

2 Purpose

This policy explains the records management arrangements adopted within Shropshire Community Health NHS Trust. It covers records prepared and maintained in all media, including paper and electronic records, for the benefit of all of Trust's stakeholders.

It describes the Trust's processes developed to achieve best working practices in the creation, use, security, storage, retention and destruction of all records produced within the organisation.

The aim of this policy is to promote a records management culture that ensures:

- **Records are available when needed:** from which the Trust is able to form a reconstruction of activities or events that have taken place;
- **Records can be accessed:** records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- **Records can be interpreted:** the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **Records can be trusted:** the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **Records can be maintained through time:** the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **Records are secure:** from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **Records are retained and disposed of appropriately:** using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **Staff are trained:** so that all staff are made aware of their responsibilities for record keeping and record management.

3 Definitions

Records Management NHS Code of Practice key definitions:

Corporate Records: Records (other than health records) that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees.

Health Record: A single record with a unique identifier containing information relating to the physical or mental health of a given patient who can be

identified from that information and which has been recorded by, or on behalf of, a health professional, in connection with the care of that patient. This may comprise text, sound, image and/or paper and must contain sufficient information to support the diagnosis, justify the treatment and facilitate the ongoing care of the patient to whom it refers.

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(E)].

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

4 Duties

The Records Management NHS Code of Practice has been published by the Department of Health as a guide to the required standards for the management of records for those who work with or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice and states that:

Chief Executives and Senior Managers 'are personally accountable for records management' and that 'all individuals who work for an NHS organisation are responsible for any records which they create or use in the performance of their duties' and 'Furthermore, any record that an individual creates is a public record'[1].

4.1 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.

4.2 Directors, Deputy Directors, Locality and Service Managers

Directors, Deputy Directors, Locality 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.

4.3 Director of Nursing, Allied Health Professionals, Quality and Workforce

The Director of Nursing, AHPs, Quality and Workforce acts as the lead for Records Management within the Trust

[1] Records Management: NHS Code of Practice (Part 1 – March 2006)

4.4 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.

4.5 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.
- 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, and supporting, the Corporate Risk Manager in records management related incidents investigations and follow up actions.
- Advising and supporting the activities of Local Records Management Leads.
- Liaising with the Local Records Management Leads, other relevant staff leads, and the IT Learning and 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.

4.6 Local Records Management Leads

Local Records Managers have been identified to represent directorates and services within SCHT. 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 be 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:

- Process for the creation of accurate records
- Records registration and tracking systems
- Systems for the safe storage of records to minimise loss
- Records are archived in appropriate, secure areas
- Retention periods defined in the Records Retention Archiving and Disposal Policy are followed
- A mechanism for identifying records which must be permanently kept

- 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 records management practices / procedures
- Advising on the training requirements of their staff, including local induction training

4.7 Caldicott Guardian

The Caldicott Guardian is responsible for approving and ensuring that appropriate protocols for the management of patient confidential information are in place. In particular they are responsible for monitoring compliance with Trust's Confidentiality Code of Practice. The Medical Director acts as the Trust's Caldicott Guardian.

4.8 Senior Information Services Manager

The Senior Information Services Manager acts as the Trust's Lead for Information Governance and Data Protection and is chair of the Information Governance Operational Group.

4.9 Managers

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 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

4.10 All 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) Record Keeping: Guidance for nurses and midwives 2009, Health Professions Council (HPC) Standards and General Medical Council (GMC) Good Medical Practice: guidance for doctors

- 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 mangers 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 to contact with patient or personal information are subject to a common law duty of confidence. This duty of confidence continues beyond the death of a patient or after an employee has left the NHS.

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

4.11 The Trust Board

The Trust Board has overall responsibility for reviewing and approving this policy.

4.12 Information Governance Committee and Operational Group

The Information Governance (IG) Committee has delegated responsibility from the Board to approve Information Governance related policies including the Records Management Policy and related policies.

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 to the IG Committee any issues of concern.

4.13 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
- Monitoring related reported incidents and agreeing appropriate action plans to address any issues identified in relation to this policy.
- Providing the Information Governance Operational Group with regular updates on any relevant incidents or related actions being carried out. Escalating incidents and issues to this group if required.

The full terms of reference for the Records Management Group can be found at Appendix 5.

5 Records Management

As stated in Records Management: NHS Code of Practice *"All NHS records are public records, under the terms of the Public Records Act 1958 sections 3*

(1)-(2)" and the processes defined in this policy covers all records produced within the Trust. Records include:

- Patient health records (electronic or paper based, including those concerning all specialties);
- Birth, and all other registers;
- Minor operations (and other related) registers;
- Administrative records (including for example, personnel, estates, financial and accounting records; notes associated with complaint-handling);

And may be in any medium including:

- X-ray and imaging reports, output and images;
- 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 (both outgoing from the NHS and incoming responses from the patient).

Records are legal documents and everyone working for the NHS has a common law duty of confidence to clients, staff and their employer. This duty of confidence continues after the death of a patient and after an employee has left the NHS.

Therefore, as good information is essential to the effective delivery of high quality evidence based health care it is anticipated that the robust implementation of this policy will help the Trust to achieve the following objectives:

- Meet legal and regulatory requirements, including requests from patients under access to health records and requests for information from the general public under freedom of information legislation
- To support patient care and continuity of care
- To support evidence-based clinical practice
- To support patient choice and control over treatment and services designed around patients
- To assist clinical and other types of audits
- To support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of material and the needs of future research
- To support day-to-day business which underpins the delivery of care
- To support sound administrative and managerial decision-making, as part of the knowledge-base for NHS services

Note: The *Clinical Record Keeping Policy* gives more in depth detailed guidance specific to health records and clinical record keeping requirements.

5.1 Records Life Cycle

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 archrival preservation. The key components of records management are:

- Record creation
- Record keeping
- Record maintenance (including tracking of record movements)
- Access and disclosure
- Appraisal
- Archiving
- Disposal or archival preservation

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

See Appendix 2 for diagram of **Record Lifecycle Management**

6 Records Creation and Registration

6.1 Record Creation

Records are created throughout the Trust to ensure that information is available for the purposes defined in the introduction of this policy.

Directorates and services will ensure accurate record keeping by the use of standardised documentation and locally agreed processes and procedures for the creation and filing of records. The information contained in records is only usable if it is accurate and legible, is kept up to date, and is easily accessible, therefore, documented local procedures are important to ensuring a high standard of data quality for both manual and electronic records.

6.2 Use of Abbreviations

It is recognised that the use of abbreviations saves time when writing documents but excessive use of abbreviations can make it hard to understand or follow the flow of the content of a document. Best practice is to only use abbreviations where necessary and to include the full term the first time it is used within that document with the abbreviation in brackets e.g. Care Quality Commission (CQC). This is of particular importance in minutes of meetings as these are evidence of topics discussed and decisions made and may be referred to by someone who does not have the knowledge and background of those who attended that meeting. Additionally when using abbreviations in business or organisational documents it is also advisable to

include a glossary at the end of the document listing all abbreviations or terms used.

6.3 Record Registration

In order to ensure records can be identified and retrieved when needed it is good practice to maintain a register and to allocate a registration system to a set of records.

Registration is the act of giving a record a unique identifier (number or alphabetical prefix) on its entry into a record-keeping system, and which records that sequentially in a register or index.

All electronic records systems used by the Trust require unique identifiers, e.g. some systems use the patient's NHS number to register their records.

Determining which records require registering is a decision that should be made by staff with advice from the Records Manager and Local Records Manager and, when relevant, the Caldicott Guardian.

The kinds of records, which are most likely to be placed on a register, include, but are not limited to:

- Care/clinical records
- Personnel records
- Corporate documents
- Policies and procedural documents
- Policy papers (reports, correspondence, etc)
- Minutes, circulated papers, etc. of meetings
- Financial papers
- Contracts and Service Level Agreements (SLAs)
- Estates papers
- Performance monitoring
- Papers relating to the preparation of legislation
- Freedom of Information and Data Protection requests
- Complaints and claims papers and correspondence
- Research and development papers.

Registration will depend on the Trust's business need to maintain accountable records of particular activities, its information needs, how many records there are on that particular topic or in that series and the obligations under the Data Protection Act, the Freedom of Information Act and other relevant legislation including Records Management: NHS Code of Practice.

It is important that all patient/client records held on a system with a Master Patient Index (e.g. EMIS, Lorenzo) have their NHS number recorded and that these numbers have been validated. For further guidance please refer to the Trust's *NHS Number Retrieval, Verification and Use Procedure*.

Best practice principles of registration are:

- The file title must be unique

- The registration identity assigned to each file must be unique
- Both must be relevant to and easily understood by all users

Registration systems, including organisational and local document registers (e.g. policies, contracts and information asset registers), should be monitored regularly and reviewed at least once every two years to ensure that they continue to operate effectively and efficiently and meet the needs of users.

It is essential that registration systems include a mechanism for avoiding duplicate records. Electronic records systems will also have an integral audit trail.

7 Procedural Documents

Approved procedural documents, including strategies, policies, protocols and guidelines record the processes by which Shropshire Community Health NHS Trust plans and conducts its activities. They are necessary to ensure that the Trust's vision and goals, as recorded in the strategic plan are achieved, that risks to these objectives are adequately mitigated, that legal and regulatory obligations are met and that the Trust's intentions and methodologies are clearly understood by all stakeholders.

The control of procedural documents is essential, not only to comply with corporate and clinical governance standards but as an essential means of ensuring standardisation in the provision of safe care across the Trust and the successful reduction of risk.

The *Policy on the Development and Management of Procedural Documents* has been developed to ensure a structured and systematic approach to the development, review, ratification, dissemination and retention of procedural documents. It establishes a framework that ensures all policies and procedures are:

- of a consistently high standard,
- up to date,
- available to all staff,
- implemented and complied with, and
- reviewed at regular intervals.

All staff involved in the design, development, approval and review of procedural documents must ensure they are aware of their responsibilities as detailed in the *Policy on the Development and Management of Procedural Documents*. For further advice and guidance contact the Corporate Risk Manager.

8 Personal Identifiable Data

Personal Identifiable Data (PID) or information about either patients or employees recorded for any purpose should not be kept for longer than is necessary. Neither should it be used for any purpose than that for which it was collected.

PID information must not be passed to on to other people without the consent of the person concerned except as permitted under the Data Protection Act 1998 or under the common law where there is an over-riding public interest. Further information is contained within the Trust's *Data Protection Policy* and *Confidentiality Code of Practice*.

When transferring PID information suitable security must be used. In the case of electronic transfer of PID information then the appropriate encryption process must be used following guidance given in the Trust's *Information Security Policy* and other relevant up to date advice that may be published from time to time.

To ensure that they are easy to read and not open to misinterpretation personal records should:

- Only state relevant and useful information.
- Be complete, factual, consistent, accurate and consecutive.
- Be written clearly, legibly and in such a manner that they cannot be erased.
- Be held securely and confidentially.
- The information contained within records should be used for the purpose for which it was obtained and only shared appropriately and lawfully.
- Be accurately dated, timed and signed. (The signatories name should be printed at the side of the first entry or be matched to an authorised signatory list).
- The use of abbreviations should be kept to a minimum. If abbreviations are used, they should be from an agreed list.
- Erasers and liquid paper should not be used to cancel errors. A single line should be used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the amendment.
- Be readable on any photocopies.
- Be bound and stored so that loss of documents is minimised.
- Identifying problems that have arisen and the action taken to rectify them.

Personal records should not include:

- Unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subjective statements.
- Personal opinions regarding the subject.
- Or be kept for longer than is necessary.

Note: The *Clinical Record Keeping Policy* gives more in depth guidance specific to personal health records.

9 Records Tracking

Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently.

One of the main reasons why records get misplaced or lost is because their next destination is not recorded anywhere.

Tracking mechanisms should record the following (minimum) information:

- The item reference number or other identifier (e.g. Staff Number).
- A description of the item (e.g. the file title).
- The person, unit or department, or place to whom it is being sent.
- The date of the transfer to them.

9.1 Manual Tracking Systems

Common methods for manually tracking the movements of active records include the use of:

- A paper register – a book, diary, or index card to record transfers.
- File "on loan" (library-type) cards for each absent file, held in alphabetical or numeric order.
- File "absence" or "tracer" cards put in place of absent files.

Manual systems often suffer because they are rarely updated, quickly rendering such systems ineffective.

9.2 Electronically Operated Tracking Systems

Automated methods of tracking include the use of:

- A computer database in place of paper/card index.
- Bar code labels and readers linked to computers.
- Workflow software to track documents electronically.

An electronic system can drastically reduce the amount of paper generated, and therefore the volume of paper to be stored. Using an electronic tracking system rather than, for example, a card index, can be more efficient – speeding up information retrieval times, reducing miss-filing, and the problems associated with the use of absence markers.

A well thought-out tracking system – manual or electronic – should meet all user needs and be supported by adequate equipment. It should provide an up-to-date and easily accessible movement history and audit trail. The success of any tracking system depends on the people using it and therefore all staff must be made aware of its importance and given adequate training and updating.

Tracking systems should be implemented and reviewed in liaison with relevant the Local Records Management Leads.

10 Storing Records

10.1 Current Records

Records in constant or regular use, or those likely to be needed quickly, should be kept near to the staff who will need them. They should be kept stored securely in lockable desk drawers or cabinets, within rooms, which should be locked when left unattended.

Less frequently used or archived records can be moved to more effective and space efficient storage options. Points to consider are:

- Appropriate environmental storage conditions.
- Mobile racking and warehouse-type units.
- Off-site secure storage and retrieval services.
- Microfilm, microfiche and digital scanners to capture and store images.
- Picture archiving for diagnostic imaging.

It is important to recognise that different record types and different storage media may require different approaches. Appropriate retrieval arrangements should be agreed before archiving, including appropriate strategies for migration of electronic information between systems. Guidance on suitable environmental conditions for electronic data storage media (as recommended in BS 4783) is available from the National Archives (www.nationalarchives.gov.uk/).

Contracts for non-NHS agencies or staff must require that patient information is stored and retrieved according to specified security and confidentiality standards and Data Protection guidelines. Records identified for permanent preservation must be stored within "places of deposit" approved by the National Archives.

Records storage areas must provide a safe working environment, with adequate space and equipment in compliance with health and safety legislation and fire regulations.

Storage areas must have sufficient capacity to accommodate records for the required minimum retention periods and to accommodate the annual growth of new records and the following factors should also be taken into account:

- Security (especially for confidential material).
- The user's needs.
- Type(s) of records to be stored.
- Their size and quantities.
- Usage and frequency of retrievals.
- Suitability, space efficiency and price.

10.2 Other Regularly Used Paper Records

As the need for quick access to particular records reduces, it may be more efficient to move the less frequently used material out of the work area and into archive storage.

When transferred into an archive, other regularly used paper records should be stored on shelves in a way that facilitates retrieval. Boxing may be required where there are risks from damage by excessive light or by flooding. Records should be stored off the floor on suitable shelving to provide some protection from flood, dampness and dust.

The width of aisles and general layout of storage areas must conform to fire, health and safety, and similar regulations.

10.3 Electronic Records

It is important that any records held electronically are filed in a consistent manner and are easily identifiable when they need to be retrieved. Where possible, electronic records should be held on network servers with appropriate permissions set to control access to those who need to access them. If records are held on a non-networked drive they should be backed up regularly when access to the network is available or to another suitable back-up device. This is of particular importance to laptop users and they must ensure the information on their laptops are regularly backed up.

When shared library / network drives (folders) are used within a service or department it is important that the folder structure reflects the business needs and that there is guidance available for all staff are aware of how to file records efficiently. Consideration on archiving and deletion of electronic records should also be included in any guidance documentation. The Records Manager can give further advice and guidance on this matter as required.

10.4 Other Non-Paper Records

Microfilm and fiche have been used for many years and Courts will accept them as evidence. Microfilming comes into its own as a relatively cost-efficient way to capture and store images of otherwise bulky or deteriorating archival material:

- To minimise storage costs of materials, which would otherwise be destroyed.
- To make copies available for other uses (such as research) whilst safeguarding the original.
- To reduce the storage space occupied by low activity paper records.

Services within the Trust will hold visual images – either as diagrammatic images and still photographs (which may be prints, negatives, slides, transparencies, and digital images) or as moving images (film or video), X-rays, telemedicine, diagnostic progress monitoring.

In the case of photographs, the quality of image available from negatives or original prints should be considered and new prints may be made in cases where the original is deteriorating.

Photograph and film collections assembled by clinical and other staff through their work within the Trust should be regarded as Public Records and subject to these guidelines. Note that the provisions of the Data Protection Act 1998 on registration of records and restriction of disclosure relate to photographs of identifiable individuals as well as to other personal records. Blanking out of eyes does not render them unidentifiable.

Film should be stored in dust-free metal cans and placed horizontally on metal shelves. Microform, sound recordings and video-tape should be stored in metal, cardboard or inert plastic containers, and placed vertically on metal shelving.

10.5 Transfer of Non Electronic Personal Identifiable Data Guidance

The transfer of all Personal Identifiable Data (PID) must satisfy current legislation and follow the NHS and Trust codes of practice, policies and guidance on the protection and use of patient / staff information.

Security and confidentiality of records should be paramount; therefore records should never be taken off site unnecessarily or without the approval of the line manager. If requesting records / PID ensure the sender has your full address details. The use of a signature block with contact details at the bottom of e-mails is strongly recommended as good practice.

When transferring PID, especially patient / staff records, staff should:

- Ensure a track and trace system is in place so that there is an audit trail of where that record is.
- Ensure it is enclosed in a folder / envelope or transported in a suitable secure container.

For further specific guidance on the transfer of PID refer to the Trust's *Information Security Policy* and the *Confidentiality Code of Practice*.

10.6 Labelling and Packaging Records for Transporting

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

- Sealed in envelopes or secure mail pouches (sealed using numbered tamper-proof seals);
- Packages must be properly addressed to a named individual and must include their role, department and location;
- Any records that may be damaged in transit must be enclosed in suitable padding or containers;
- 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.

There are various options if records are to be mailed, such as recorded delivery, registered mail etc or are to be sent by Internal Transport, in staff vehicles, by courier or exceptionally by taxi. When choosing options staff should consider the following:

- Will the records be protected from damage, unauthorised access or theft?
- Consider the use of double envelopes with the outside envelope fully addressed as normal and the inside envelope also addressed but used as additional protection and may have specific instructions e.g. "Only to be opened by …."
- Is the level of security offered appropriate to the degree of importance, sensitivity or confidentiality of the records?
- Does the mail/courier provider offer 'track and trace' options and is a signature required on delivery?

10.7 Handling and Transporting Records

Because it is essential that records remain legible and usable:

- No-one handling, using or transporting records should eat, drink or smoke near them.
- People using sensitive records should not leave them unattended on desks. Particularly they should not be left exposed to the view of unauthorised staff, patients, other clients or the public.
- Personal records being carried on a site e.g. from the archive storage to a department, should be enclosed in an envelope, secure mail pouch or secure box.
- Records should be handled carefully when being loaded, transported or unloaded. Records should **never** be thrown.
- Records should be packed carefully into vehicles or on trolleys to ensure that they will not be damaged by the movement of the vehicle.
- Vehicles must be fully covered so that records are protected from exposure to weather, excessive light and other risks such as theft.
- No other materials that could cause risks to records (such as chemicals) should be transported with records.
- Vehicles containing records should be locked when unattended.
- Records being transported should always be kept out of sight.

10.8 Taking Records Off Site

Security and confidentiality of records should be paramount. Therefore records should never be taken off site unnecessarily or without the approval of the line manager.

It is essential that any such records are tracked out of the respective department so that other staff are aware of the location of the record. If records are taken home, they must be stored securely and in accordance with the staff member's Professional Code of Conduct.

Records should not be left in vehicles overnight.

The Records Manager and Local Records Managers can provide advice on the precautions to take. For further guidance refer to the Trust's Information Security Policy.

11 Records Retention Archiving and Disposal

All records held by the Trust will be retained, archived and disposed of in accordance with guidance given by the Department of Health in 'Records Management: NHS Code of Practice' Parts 1 and 2. The Trust's *Records Retention, Archiving and Disposal Policy* details processes and procedures to be followed. In summary:

11.1 Records Retention

The length of the retention period depends upon the type of record and its importance to the business of the Trust. Whilst the destruction of records is irreversible the cost of keeping them can be high and recurring.

Retention periods apply to the master (primary) copy of documents not copies (secondary) produced for reference.

Records should be retained for the minimum period stated in the Retention schedule section of the *Records Retention Archiving and Disposal Policy*.

Where records are not mentioned in this schedule or new types of record are developed, the Department of Health or the National Archives will be consulted.

Where it is proposed that records will be retained for a period other than that specified in the NHS Retention & Disposal Schedule this should be reported to the Records Manager for approval by the Records Management Group.

Advice on the retention of records can be obtained from the Records Manager, Local Records Managers, the Caldicott Guardian or the Senior Informatics Manager.

11.2 Records Disposal

Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy such records is fully effective and secures their complete illegibility. Normally this will involve shredding, pulping, or incineration.

Floppy disk/CD/backup tapes/audio tapes containing identifiable information must be reformatted with a random pattern to ensure data cannot be recovered or they must be physically destroyed. Removable media such as floppy disks, CDs, memory sticks and hard drive units must also be destroyed. This can be done on site, or via an approved contractor. Guidelines are contained within the Trust's *Information Security Policy* and advice can be sought from the Informatics Department at William Farr House.

11.3 Confidential Waste

It is important that, when required, confidential records are destroyed in a secure manner. If the volume is minimal and a document shredder is used it must be, at minimum, a cross-shred version. With larger volumes of confidential waste suitable secure, labelled containers must be used. These should then be disposed of using a confidential waste contractor. Where practical, this service should be carried out onsite and monitored by an appropriate member of staff. A certificate of destruction must be obtained by the person responsible for contracting these bulk destructions services as evidence that the confidential waste has been disposed of securely. They should also maintain a log of the destruction of confidential waste.

11.4 Archiving Records

Archived records must be stored in a secure location in accordance with the Storing Records section of this policy and guidance given in the Trust's *Records Retention, Archiving and Disposal Policy*.

12 Transfer of Records to Other Organisations

Records transferred to other organisations must be transferred in entirety to organisations that have a legitimate need for them. Therefore, care should be

taken to include all documents in a record including those that have been scanned. Accurate tracking of these records is essential.

Local procedures will need to be documented and approved for and regular transfers and specific circumstances.

13 Consultation

This procedure has been developed by the Records Manager in consultation with representatives from services and departments 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 and administrative leads. The procedure has also been presented to the Information Governance Operational Group before submission to the Information Governance Committee for final ratification.

14 Dissemination

These guidelines will be disseminated by the following methods:

- Published to the Website
- Directors/Senior Managers – to disseminate within their areas
- Staff - via newsletters/team briefings
- Awareness raising by Records Manager and Local Records Management Leads

15 Advice and Training

15.1 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@shropcom.nhs.uk

Caldicott Guardian

Dr Alastair Neale

Tel: 01743 277500, E-mail:alastair.neale@shropcom.nhs.uk

Senior Information Services Manager (IG Lead and Data Protection Officer)

Chris Berry

Tel: 01743 871951, E-mail: chris.berry@shropcom.nhs.uk

15.2 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*. Section 5 – Training Approach; Section 7 – Monitoring Compliance; Appendix One – Mandatory Training (TNA) Matrix

For further information contact:

Deborah Hammond - IT Training Learning & Development Team Manager
Tel: 01743 276670, E-mail: deborah.hammond@shropcom.nhs.uk

16 Review

This policy will be reviewed every two years by the Records Manager, liaising with the Records Management Group to ensure the content remains relevant and up to date and reflects any changes in legislation, standards and professional codes of practice.

17 Compliance Monitoring

To achieve compliance with the Care Quality Commission, the NHS Litigation Authority's Risk Management Standard and the Information Governance Toolkit requirements regular audits of record keeping standards and practice will be undertaken, co-ordinated by the Records Manager.

Note: For specific details on monitoring related to health records refer to the monitoring section of the *Clinical Record Keeping Policy*.

17.1 Records Audits

The Records Manager will co-ordinate the audit of records management systems, processes and records liaising with the Clinical Audit Team and appropriate committees/groups to ensure the audits:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of the records management audits will be reported initially to the Records Management Group then to the Information Governance Operation Group for further dissemination to other committees/groups as required e.g. Quality and Safety Operational Group, Information Governance Committee, Quality and Safety Committee and the Audit Committee.

17.2 Incident Reporting

Compliance monitoring will also be undertaken by the Risk Management Team and the Records Manager scrutinising reported incidents and near misses that relate to record keeping in accordance with the Incident Reporting Code of Practice. They will ensure remedial actions are taken and report findings initially to the Records Management Group and then to the Information Governance Operation Group and other relevant committees/groups, managers and members of staff as required.

18 References

The following documents were used to prepare this strategy:

- The Data Protection Act, 1998
- The Freedom of Information Act, 2000
- Human Rights Act 1998
- The Public Records Act, 1958
- The Access to Health Care Records Act, 1990
- The Access to Medical Records Act, 1998
- Care Quality Commission – Essential standards for quality and safety - Records (Regulation 20 and Outcome 21) – http://www.cqc.org.uk/sites/default/files/media/documents/gac_-_dec_2011_update.pdf
- NHS Litigation Authority Risk Management standards – http://www.nhsla.com/RiskManagement/
- NHS CFH – Information Governance Toolkit requirements – https://www.igt.connectingforhealth.nhs.uk/
- NHS Records Management – Code of Practice – http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747
- Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 – http://www.justice.gov.uk/guidance/docs/foi-section-46-code-of-practice.pdf
- The National Archives website – Standards and best practice for records managers – http://www.nationalarchives.gov.uk/information-management/projects-and-work/standards-records-managers.htm
- The National Archives – Records Management Standard, RMS 1.1 File Creation - http://www.nationalarchives.gov.uk/documents/stan_file_creation.pdf
- NHS Confidentiality Code of Practice – http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550
- The Care Record Guarantee – http://www.nhscarerecords.nhs.uk/security
- Your Health Information, Confidentiality and the NHS Care Records Service – www.nhscarerecords.nhs.uk

For a brief explanation of the contents of the primary reference documents see **Appendix 1**

19 Related Documents

Shropshire Community Health NHS Trust policies and procedures which relate to this policy include:

- Clinical Record Keeping Policy
- Records Retention, Arching and Disposal Policy
- NHS Number Retrieval, Verification and Use Procedure

- Policy on the Development and Management of Procedural Documents
- Information Security Policy
- Information Governance Policy
- Information Quality Assurance Policy
- Information Risk Policy
- Data Protection Policy
- Freedom of Information Policy
- Confidentiality Code of Practice
- Incident Reporting Policy
- Mandatory Training Policy and Procedure

These documents are available on the Trust's website http://www.shropshire.nhs.uk/shropscommunityhealth/Staff-Zone/Policies/

20 Glossary

20.1 Definitions

Word	Definition	Source
Archive	Those records that are appraised as having permanent value.	National Archives
Caldicott Principles	Six principles that should be followed when considering sharing confidential information, put together by Dame Fiona Caldicott following a review she carried out in regard to confidentiality in 1997	
Classification	The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system. (BS ISO 15489-1:2001(E))	NHS Code of Practice
Corporate Record	A document becomes a record when it has been finalised and becomes part of the organisation's corporate information (a document has content – a record has content, context & structure)	Information Governance Toolkit – Corporate Governance
Disposal	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	National Archives

Word	Definition	Source
	institution). They may also include the movement of records from one system to another (for example paper to electronic).	
Electronic Staff Record (ESR)	This is the national, integrated Human Resources (HR) and Payroll system which will be used by all 600+ NHS organisations throughout England and Wales.	Electronic Staff Record Website
Encryption	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 that 64-bit.	Get Safe Online Organisation
Filing System	A plan for organising records so that they can be found when needed. (The National Archives, Records Management Standard RMS 1.1)	NHS Code of Practice
Index cards	A series of cards that may be arranged alphabetically for the purpose of facilitating references to names, file titles, etc or numerically for file references.	National Archives
Indexing	The process of establishing access points to facilitate retrieval of records and/or information. (BS ISO 15489-1:2001(E))	NHS Code of Practice
Information Commissioner	The Information Commissioner enforces and oversees the Data Protection Act 1998 and the Freedom of Information Act 2000.	NHS Code of Practice
Jointly Held Records	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.	NHS Code of Practice
Master Patient Index (MPI)	(i) 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 Person Index are used interchangeably.	NHS Code of Practice
Master Patient Index (MPI)	(ii) Index referencing all patients relating to an area or organisation and acting as a source of patient /service user demographic data for other linked services and systems	NHS Information Standards Board

Word	Definition	Source
NHS Care Records Service	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.	NHS Code of Practice
NHS Number	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.	NHS Code of Practice
NHS Record	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.	NHS Code of Practice
Personal Identifiable Data (**PID)**	Personal Identifiable 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.	
Protective Marking	The process of determining security and privacy restrictions on records. Previously called 'classification'.	NHS Code of Practice
Publication Scheme	A publication scheme is required of all NHS organisations under the Freedom of Information Act. It details information which is available to the public now or will be in the future, where it can be obtained from and the format it is or will be available in. Schemes must be approved by the Information Commissioner and reviewed periodically to make sure they are accurate and up to date.	NHS Code of Practice

Word	Definition	Source
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)	NHS Code of Practice
Records System / Record Keeping System	An information system which captures, manages and provides access to records through time. (The National Archives, Records Management: Standards and Guidance – Introduction Standards for the Management of Government Records) Records created by the organisation should be arranged in a record-keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information. Record-keeping systems should contain descriptive and technical documentation to enable the system and the records to be understood and to be operated efficiently, and to provide an administrative context for effective management of the records, including a documented set of rules for referencing, titling, indexing and, if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information and to maintain security and confidentiality.	NHS Code of Practice
Referencing	A referencing system helps to provide a means of identifying and retrieving records. Can be used when creating a register or index of records. Several types of referencing can be used: Alphabetical, Numerical, Alphanumeric or Keyword.	National Archives
Register	A list of records, usually in simple sequence such as date and reference number, serving as a finding aid to the records.	National Archives
Registration	Registration is the act of giving a record a unique identifier on its entry into a record-keeping system.	NHS Code of Practice
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.	NHS Code of Practice
Tracking	Creating, capturing and maintaining information about the movement and use of	NHS Code of

Word	Definition	Source
	records. (BS ISO 15489-1:2001(E))	Practice
Transfer of Records	Transfer (custody) – Change of custody, ownership and/or responsibility for records. (BS ISO 15489-1:2001(E)) Transfer (movement) – Moving records from one location to another. (BS ISO 15489-1:2001(E)) 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.	NHS Code of Practice
Version Control	The management of multiple revisions to the same document that enables one version of a document to be identified from another.	National Archives

20.2 Abbreviations

Term / Abbreviation	Definition / description
AHPs	Allied Health Professionals
CQC	Care Quality Commission
DH	Department of Health
DfE	Department for Education
DPA	Data Protection Act
ESR	Electronic Staff Record
FOI	Freedom of Information
GMC	General Medical Council
ICO	Information Commissioner's Office
IG	Information Governance
IGT	Information Governance Toolkit
IM&T	Information Management and Technology
MCA	Mental Capacity Act
MPI	Master Patient Index
NHS CRS	NHS Care Records Service
NHSLA	NHS Litigation Authority
NMC	Nursing and Midwifery Council
PALS	Patient Advice and Liaison Service
PID	Personal Identifiable Data
SCHT	Shropshire Community Health NHS Trust

Appendix 1: Reference Documents

Records Management: NHS Code of Practice Part 1 and 2

This document, which was published on 30th March 2006 with Part 2 being revised in January 2008 and can be found on the Department of Health website gives guidance '….on the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England' and '..is based on current legal requirements and professional best practice'.

This document:

- Establishes an information governance framework for NHS records management in relation to the creation, use, storage, management and disposal of all types of records;
- Clarifies the legal obligations that apply to NHS records;
- Explains the actions required by Chief Executives and other managers to fulfil these obligations;
- Explains the requirement to select records for permanent preservation;
- Sets out recommended minimum periods for retention of all types of NHS records, regardless of the media on which they are held; and
- Indicates where further information on records management may be found.

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

The Data Protection Act 1998

This act provides legislation regarding the protection and use of information about identifiable living individuals. It gives seven rights to individuals in respect of their own personal data held by others, they are:

- Right of subject access;
- Right to prevent processing likely to cause damage or distress;
- Right to prevent processing for the purpose of direct marketing;
- Rights in relation to automated decision taking;
- Right to take action for compensation if the individual suffers damage;
- Right to take action to rectify, block, erase or destroy inaccurate data; and
- Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

Those who decide how and why personal data are processed (data controllers), must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act.

The Freedom of Information Act 2000

The access provisions of this act replace the access provisions for public records set out in the Public Records Act 1958-67 and became effective from January 2005. This act provides legislation regarding access to information held by public authorities. Any person making a request for information to a public authority is entitled:

- To be informed in writing by the public authority whether it holds information of the description specified in the request, and
- If that is the case, to have that information communicated to him.

Requests for information must be dealt with promptly and usually within 20 working days. The first day of the 20 is the first working day after the request was received.

The Lord Chancellor issued two Codes of Practice under the Act. The section 45 code sets out good practice in handling requests for information and includes a section on public sector contracts. The section 46 code sets out good practice in records management and for the transfer of public records.

The Caldicott Report

In March 1996, guidance on The Protection and Use of Patient Information was published by the Department of Health. This guidance required that when the use of patient information was justified, only the minimum necessary information should be used and it should be anonymised wherever possible. In the light of that requirement the Chief Medical Officer established the Caldicott Committee to review the transfer of all patient-identifiable information from NHS organisations to other NHS or non-NHS bodies for purposes other than direct care, medical research or where there is a statutory requirement, to ensure that current practice complies with the Departmental guidance.

On completion of the work, the committee concluded that, whilst there was no significant evidence of unjustified use of patient-identifiable information, there was a general lack of awareness throughout the NHS of existing guidance on confidentiality and security, increasing the risk of error or misuse.

The Caldicott committee's report, published in December 1997, contained 16 recommendations, which related to ensuring best practice in the use of information flows between organisations. These included the requirement of NHS bodies to appoint a Caldicott Guardian.

The Caldicott Principles are:

1. Justify the purpose of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum required
4. Access should be on a strict need-to-know basis
5. Everyone must understand their responsibilities
6. Understand and comply with the law

Information Sharing: Guidance for Practitioners and Managers (2008)

Guidance on information sharing which relates closely to Caldicott topics can be found on the Department for Education (DfE) document[2]. In particular, the **Information Sharing: 7 Golden Rules** are broadly the same as the Caldicott principles but have the added benefit that they were specifically developed for sharing information across organisations

1. Remember that the Data Protection Act is not a barrier to sharing information
2. Be open and honest
3. Seek advice
4. Share with consent where appropriate
5. Consider safety and well-being
6. Necessary, proportionate, relevant, accurate, timely and secure
7. Keep a record

NHS Litigation Authority: Risk Management Standards

The NHS Litigation Authority provides 'insurance' for NHS bodies against both clinical negligence and estates based risk. Compliance with the requirements of the standard result in reduced payments to the authority.

For further details on the NHSLA Risk Management Standards for NHS Trusts providing Acute, Community, or Mental Health & Learning Disability Services and Independent Sector Providers of NHS Care: http://www.nhsla.com/riskmanagement

Information Governance Toolkit

The Information Governance Toolkit (IGT) was produced jointly by the Department of Health and the NHS Information Authority and represents Department of Health policy. To assist in achieving compliance with the initiatives the IGT presents the various items as a series of easy to follow requirements against which the Organisation's current and planned attainment levels can be identified. The Information Governance Toolkit covers the required areas as a set of six initiatives or work areas:

1. Information Governance Management
2. Confidentiality and Data Protection Assurance
3. Information Security Assurance
4. Clinical Information Assurance
5. Secondary Uses Assurance
6. Corporate Information Assurance

For a full list of the Information Governance Toolkit requirements for Community Health Providers:
https://nww.igt.connectingforhealth.nhs.uk/RequirementsList.aspx?tk=410653724337297&lnv=2&cb=13fa318d-eec2-4103-9500-57f3a1f44f9f&sViewOrgType=25&sDesc=Community%20Health%20Provider

[2] Available from the Department of Education website: http://www.education.gov.uk/childrenandyoungpeople/strategy/integratedworking/a0072915/information-sharing

Care Quality Commission – Essential standards for quality and safety

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 CQC continuously monitor compliance with essential standards as part of a new, more dynamic, responsive and robust system of regulation. Their assessors and inspectors frequently review all available information and intelligence they hold about a provider. As part of this process they also seek information from patients and public representative groups, and from organisations such as other regulators and the National Patient Safety Agency.

The CQC: Guidance about compliance Essential standards of quality and safety – March 2010 is designed to help providers of health and adult social care to comply with the Health and Social Care Act 2008 (Regulated Activities) Regulations 2010, and the Care Quality Commission (Registration) Regulations 2009. These regulations describe the essential standards of quality and safety that people who use health and adult social care services have a right to expect.

Link: http://www.cqc.org.uk/sites/default/files/media/documents/gac_-_dec_2011_update.pdf

Access to Health Records Act 1990

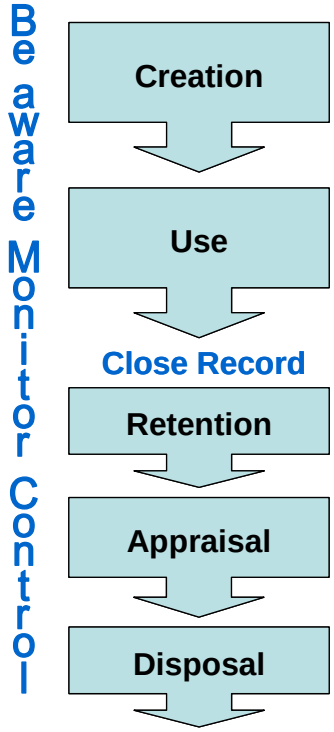
This act give the subjects of information access rights to all records irrespective of when they were created, although under section 30 access to some health, education and social work data may be constrained or denied.

While the Data Protection Act 1998 supersedes the Access to Health Records Act 1990 for living individuals, the 1990 Act remains relevant for access to information about the deceased. It provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.

Mental Capacity Act 2005

The Mental Capacity Act 2005, covering England and Wales, provides a statutory framework for people who lack capacity to make decisions for themselves, or who have capacity and want to make preparations for a time when they may lack capacity in the future. It sets out who can take decisions, in which situations, and how they should go about this. The Act received Royal Assent on 7 April 2005 and came into force during 2007. The legal framework provided by the Mental Capacity Act 2005 is supported by the Mental Capacity Act 2005 Code of Practice, which provides guidance and information about how the Act works in practice. The Code has statutory force, which means that certain categories of people have a legal duty to have regard to it when working with or caring for adults who may lack capacity to make decisions for themselves.

Appendix 2: Record Lifecycle Management



The need to Create and record accurate and complete information. Including the use of the **NHS Number** in clinical records

Handle in accordance with the legislation, guidelines and policies e.g. *Data Protection Act, Freedom of Information Act, Caldicott Principles, Healthcare Standards, Records Management NHS Code of Practice*

After closure, keep and maintain records in line with NHS recommended retention periods*

Determine whether records are worthy of permanent, archival preservation (e.g. in Hospital and University libraries, The National Archives etc)

Dispose of securely in line with national guidelines*

**Records Management NHS Code of Practice – Part 2*

Appendix 3: Contacts for Support and Advice on Records Management

Name	Title	Telephone number
Maggie Bayley	Director of Nursing, AHPs, Quality and Workforce	01743 277587
Martine Tune	Deputy Director of Nursing and Quality	01743 277500
Dr Alastair Neale	Caldicott Guardian	01743 277500
Chris Berry	Senior Information Services Manager	01743 871951
Peter Foord	Corporate Risk Manager	01743 277661
Soma Moulik	Freedom of Information Manager	01743 277500 Ext 2038
Alan Ferguson	Records Manager and Quality Facilitator	01743 277617

The National Archives

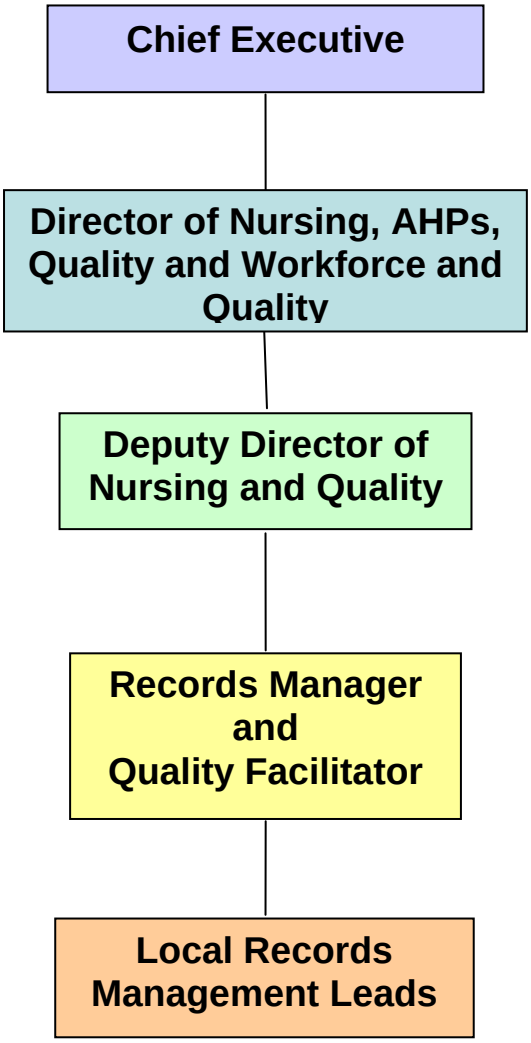
The National Archives will provide advice about records requiring permanent preservation. The website contains specific advice on Freedom of Information.

Contact details:

The National Archives,
Kew,
Richmond,
Surrey.
TW9 4DU
Tel: 020 8876 3444

www.nationalarchives.gov.uk (An e-mail contact form is available on the website)

Appendix 4: Records Management Organisational Structure



Appendix 5: Records Management Group Terms of Reference

Records Management Group
Terms of Reference

Version: 1.1 Final

Approved by: Information Governance Operational Group **Date:** 01 March 2012

Date Approved	
Date issued:	01 March 2012
Review date:	01 March 2013

Document History:	
Version:	1.1
Ratified by:	Information Governance Operational Group
Date ratified:	01 March 2012
Name of author(s):	Alan Ferguson, Records Manager and Quality

Name of responsible committee/individual: Records Management Group

Target audience: Information Governance Operational Group
Information Governance Committee
All Shropshire Community Health NHS Trust Staff

Contents

1. Introduction

The Records Management Group is a sub-group of the Information Governance (IG) Operational Group which in turn is reports to the Information Governance Committee. Its powers are delegated by the IG Committee and detailed in these terms of reference. The aim of the group is to provide assurance to the Information Governance Operational Group that the Trust has robust internal corporate and clinical records management processes. The group will undertake key functions required of the records management functions of the Trust. The group will also provide assurance that the Trust meets the standards of external regulatory bodies. Task and Finish Groups will be convened as required to cover specific records related requirements e.g. Clinical Documentation Group. The Terms of Reference for these groups will be based on the Task and Finish Group Terms of Reference in Appendix 1.

2. Constitution

The Records Management Group is a sub-committee of the Information Governance Operational Group and has no executive powers other than those specifically delegated in these Terms of Reference.

3. Membership

The membership will comprise of Local Records Leads and Representatives from services and departments across the Trust, covering both clinical and administrative areas, and will be chaired by the Records Manager and Quality Facilitator. Membership will include:

Service Delivery:

Children's and Specialist Services:

- Child Health Team
- Child and Adolescent Mental Health (CAMHS)
- Paediatric Psychology

- Children's Therapy Support Services
- Health Visiting
- Family Nursing Partnership
- School Nursing
- Health Improvement / Help 2 Quit
- Safeguarding Children and Young People
- Dental Services
- Prisons and Community Substance Misuse
- Sexual Health Services

Integrated Community Services:

(Representation covering North Shropshire Locality, Shrewsbury and Atcham Locality, Telford & South East Locality & South West Shropshire Locality)

- Community Nursing
- Interdisciplinary Teams
- Physiotherapy
- Occupational Therapy
- Enhanced Care Managers
- Community Hospitals
- Diagnostics, Assessment and Access to Rehabilitation and Treatment (DAART)
- Minor Injuries Unit (MIU)
- Advanced Primary Care Services (APCS)
- Diabetes Specialist Nursing*
- Shropshire Wheelchair and Posture Services
- Community Equipment Services

Corporate / Organisational

- Corporate Affairs
- Finance and Performance Management
- Workforce (HR)
- Occupational Health Service
- Learning & Development Team*
- Library & Knowledge Services
- Patient Advice and Liaison (PALS) & Freedom of Information (FOI) Manager
- Information Services/Informatics
- Website Developer / Administrator
- Records Manager and Quality Facilitator (Chair)

*On Records Management Group distribution - attend meetings on request

Other staff members shall be invited to attend when the Group is discussing areas of records management that are the responsibility of that staff member and where they are not already represented.

4. Meetings and Quorum

Quorum: The quorum arrangement for the Records Management Group requires the presence of at least the Records Manager or the delegated deputy and representation from the Corporate/Organisations and Service Delivery areas. There must be a minimum representation of seven members.

Members are encouraged to send a representative if they are not able to attend in person.

If the group is not quorate the meeting may be postponed at the discretion of the Chair. If the meeting does take place and is not quorate, no decision shall be made at that meeting and such matters must be deferred until the next quorate meeting.

Frequency: Meetings shall be held every two months

Members are expected to attend all meetings. However, as a minimum, members should attend at least two thirds of all meetings per year.

5. Authority

The Records Management Group has no executive powers other than those specifically delegated in these terms of reference. The Group is authorised by the Information Governance Operational Group to investigate any activity within its terms of reference. It is authorised to seek any information it requires from any employee and all employees are directed to co-operate with any request made by the Group.

In addition, the Group is authorised to seek advice from external advisors.

6. Role and Duties of the Records Management Group

The duties of the Group are to provide assurance to the Information Governance Committee via the Information Governance Operational Group relating to:

- Compliance with the relevant Information Governance standards as detailed in the Information Governance (IG) Toolkit and to act as a forum for discussion of the implementation of actions identified by this process.
- Compliance with the relevant sections of the Care Quality Commission (CQC) “Essential Standards for Quality and Safety” and to act as a forum for discussion of the implementation of actions identified by this process.
- Compliance with the relevant NHS Litigation Authority (NHSLA) Risk Management standards and to act as a forum for discussion of the implementation of actions identified by this process.
- Receiving and reviewing national records management guidance and implications for the Trust.
- The development and implementation of a Records Management Policy that complies with the relevant legislation, standards and Department of Health requirements.

- The preparation of policies, codes of practice and guidelines to support the Records Management Policy.
- Review and advise on the contents of records management related documents (e.g. policies, procedures and forms) prior to recommendation to appropriate groups
- Provide a forum for open discussion of records management issues across the Trust.
- Discuss, identify and share learning points identified from records management related incident reports, including significant events and purple cards.
- Provide support and guidance on Records Management related training delivered across the Trust
- Approval and review of sub-groups terms of reference to ensure their function is clear and meets the requirements of the Trust in delivering duties to comply with requirements.
- Receipt and review of minutes from sub-groups/committees as agreed in the annual reporting schedule.
- Monitoring progress of implementation of service development plans to ensure where required actions are need to improve Records Management these are implemented in a timely and appropriate manner
- Agree and escalate key issues/ risks of concern that cannot be addressed by the Records Management Group to the Information Governance Group
- Provide regular feedback to the Information Governance Operational Group on activity of the group to ensure appropriate assurance.

7. Monitoring Effectiveness

Through receipt of the minutes the Information Governance Operational Group monitor the effectiveness of the Records Management Group.

A record of the frequency of attendance by members, quoracy and the frequency of meetings will be maintained. Any areas of concern will be highlighted to the Chair of the Information Governance Operational Group.

8. Administrative Arrangements

The Group will receive appropriate administrative support. Duties will include:

- Preparing and circulating the agenda and papers with the Chair.
- Maintaining accurate records of attendance, key discussion points and decisions taken and issue necessary action logs within five full working days of the meeting.
- Drafting minutes for circulation to members within five full working days of the meeting.
- Maintaining a database of any documents discussed and/or approved and recall them to the Committee when due.
- Organising future meetings.
- Filing and maintaining records of the work of the Group.

9. Relationships and Reporting

The minutes of the Records Management Group will be submitted to the Information Governance Operational Group. The Chair of the Records Management Group shall draw to the attention of that Group any issues that require escalating.

The Records Management Group will report to the Information Governance Operational Group quarterly on its work in support of compliance with required Information Governance, CQC Essential Standards and NHS Litigation Authority Risk Management standards.

As a member of the Quality and Safety Operational Group the Records Manager will also feedback and follow up any actions or issues that are relevant to this group.

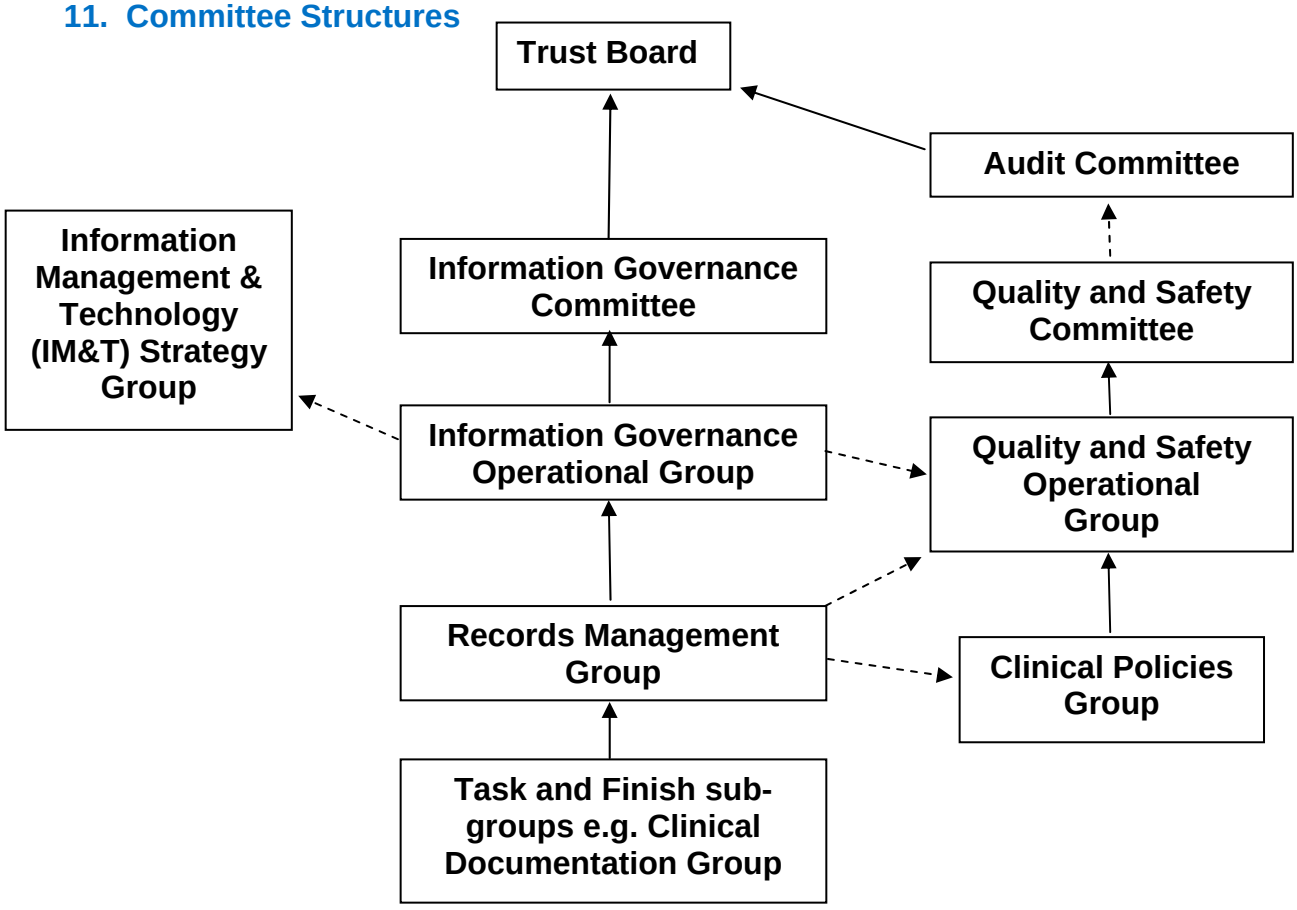
The Records Manager will also liaise with the Chair of the Clinical Policies Group to link in with any records management related topics.

The key sub-group that will report to this group is the Clinical Documentation Group with additional records management sub-groups instigated in order to cover specific records management projects or areas of concern.

10. Review of Terms of Reference

This document will be reviewed annually or sooner if agreed by the Information Governance Operational Group. Any amended Terms of Reference will be approved by the Information Governance Operational Group.

11. Committee Structures



Appendix 1: Records Management Task & Finish Groups Terms of Reference

1. Introduction

The Task and Finish Groups will be a sub-group of the Records Management Group convened in order to investigate, support and resolve a specific records management related topic or requirement.

2. Constitution

The Task and Finish Groups are a sub-committee of the Records Management Group and has no executive powers.

3. Membership

Membership and Chair of the group will be nominated and approved by the Records Management Group.

4. Meetings and Quorum

Quorum: The quorum arrangement for the Task and Finish Groups will be the Chair and two other members.

Frequency: The frequency of the meetings will be decided by the Records Management Group

5. Authority

The Task and Finish Groups will be authorised by the Records Manag3ement Group to investigate any activity within its terms of reference.

6. Role and Duties of the Task & Finish Groups

- Investigate, support and resolve the tasks identified by the Records Management Group
- Ensure that any documentation developed as part of the task meet the organisational guidelines and standards
- Identify any additional Records Management policy, procedural or process recommendations including training requirements and report to the Records Management Group
- Provide regular feedback to the Records Management Group on activity of the group to ensure appropriate assurance
- Agree and escalate key issues/ risks of concern that cannot be addressed by the Task and Finish Group to the Records Management Group

7. Monitoring Effectiveness

Through receipt of the minutes and reports the Records Management Group monitor the effectiveness of the Task and Finish Groups.

8. Administrative Arrangements

The Task and Finish Groups will provide their own administrative support ensuring agendas, minutes and relevant papers are distributed to group members in time for meetings and that copies of these are submitted to the Records Manager who will maintain a master folder of each group's documentation.

9. Relationships and Reporting

The group will report directly to the Records Management Group but will liaise with other appropriate groups in order to fulfil the tasks in hand.

10. Review of Terms of Reference

These Terms of Reference will be reviewed as part of the Records Management Terms of Reference review undertaken by the Information Governance Operational Group.