Royal Cornwall Hospitals
NHS Trust

Management of Information, Records and Data Quality Policy

V5.0

May 2024

Table of Contents

Data Protection Act 2018 (UK General Data Protection Regulation – GDPR) Legislation.

The Trust has a duty under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 to ensure that there is a valid legal basis to process personal and sensitive data. The legal basis for processing must be identified and documented before the processing begins. In many cases we may need consent; this must be explicit, informed, and documented. We cannot rely on opt out, it must be opt in.

Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 is applicable to all staff; this includes those working as contractors and providers of services.

For more information about your obligations under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 please see the Information Use Framework Policy or contact the Information Governance Team.

Royal Cornwall Hospital Trust rch-tr.infogov@nhs.net

1. Introduction

1.1. Records of NHS organisations are public records as laid down in Schedule 1 of the Public Records Act 1958. This includes records controlled by NHS organisations under contractual or other join arrangements, or as inherited legacy records of defunct NHS organisations and applies regardless of the format of the record.

1.2. The Public Records Act 1958 requires that all public bodies have effective management systems in place to deliver their functions. For health and social care, the primary reason for managing information, records and data quality is for provision of high-quality care. The Secretary of State for Health and all NHS organisations have a duty under this Act to make provisions for the security and eventual disposal of all types of records.

1.3. The principal legislation governing the management of records is Section 46 of the Freedom of Information Act 2000 (FOIA), in which it directs organisations covered by the Act to have records management systems in place which will help them to perform their statutory function.

1.4. The FOIA2000 and the DPA18 will have records management codes of practice that recommend the systems and policies that must be in place to comply with the law. Other legislation requires information to be held as proof of an activity against the eventuality of a claim.

1.5. Information, records, and data quality management is the process by which an organisation manages all aspects of recorded corporate/business/clinical information whether internally or externally generated, in any format or media type, from their creation and throughout their lifecycle to their eventual disposal. Document and archives, including those held within electronic systems, are also recorded information, and encompassed by the discipline of information, record, and data quality management.

Corporate and clinical information form part of the Trust's corporate memory, providing evidence of actions and decisions and representing a vital asset supporting daily functions, operations and care delivered. They protect the interests of the Royal Cornwall Hospital NHS Trust and the rights of patients, staff and members of the public who have dealings with the Trust. They support consistency, continuity, efficiency, and productivity and help us deliver our services in consistent and equitable ways.

1.6. Personal identifiable data (PID) must be managed in accordance with this policy and commensurate with current legislation, clinical and operational needs, this includes photography, images, voice recordings and video.

1.7. Robust and governed management of information and records ensures compliance with legislative and externally monitored standards. This policy is based upon the Records Management Code of Practice for Health and Social Care and also upon current legal requirements and professional best practice.

1.8. The Trust requires accurate, complete, timely, relevant, and standardised information in order to support both the delivery of its core business objectives and the monitoring of activity and performance for internal and external management purposes. A vital pre-requisite to the production of robust information is the availability of high-quality data across all areas of the Trust.

1.9. The Data Quality Maturity Index (DQMI) which is published by NHS Digital, is intended to highlight the importance of data quality in the NHS. It provides the Trust with timely and transparent information about its data quality. The DQMI is based on completeness and validity of core data items agreed by the National Information Board (NIB) Working Group and includes such data items as NHS number, date of birth, gender, postcode, specialty, and consultant.

1.10. The Data Quality Delivery Statement issued by NHS Digital, documents that the Trust should strive to:

"Create a culture and understanding in staff of the value of capturing high quality data in real time to improve patient care. To continually record accurate data to ensure high quality care to all patients, citizens, and stakeholders"

1.11. The requirement for accurate data has increased over recent years as a result of a number of factors, including an increasing emphasis from central NHS management on the setting of performance targets. These have included requirements for waiting list and waiting time reductions and the requirement for 'clean' data for transfer to new systems. The Data Protection Act of 2018 also sets the legal requirements for data users to ensure that personal data is being kept accurate and up to date as one of its fundamental underlying principles.

1.12. Compliance with this policy will assist in implementing the recommendations from the Mid Staffordshire NHS Foundation Trust Public Inquiry relating to records management and transparency.

1.12.1. Records Management Code of Practice for Health and Social Care.

1.12.2. Records Management: NHS Code of Practice: Parts 1 and 2: 2006, revised 2009.

1.12.3. HSC 1999/053 – For the Record.

1.12.4. HSC 1998/217 – Preservation, Retention and Destruction of GP.

1.12.5. General Medical Services Records Relating to Patients (Replacement for FHSL (94) (30)).

1.12.6. HSC 1998/153 – Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice.

1.13. This policy supports the Trust's vision, 'Aspiring to provide Outstanding Care to One+All' and will achieve this through three goals:

- ✓ Goal One: Safe, High-Quality Care - Always providing safe, effective, and compassionate care, where we listen and learn to provide an excellent patient experience and reduce avoidable harm.

- ✓ Goal Two: Supported and Valued People – Working together in a supportive environment to attract, develop and retain brilliant people.

- ✓ Goal Three: Journey of Improvement – Instilling a culture of quality improvement where everyone feels empowered to make changes for the benefit of our patients.

1.14. This version supersedes any previous versions of this document.

2. Purpose of this Policy/Procedure

2.1. The purpose of this policy is to establish a framework for the Trust in how it will manage its business and clinical information and records effectively and to ensure that procedures are in place for the creation, use, tracking, retrieval, storage, management of authentic, reliable, and useable records, capable of supporting business functions and activities for as long as they are required, in whatever format and media they are presented.

2.2. This policy will underpin and support the delivery of the Digital Strategy; in particular part two which is moving the Trust to a single integrated patient record system which will enable the rationalisation of the Trust's many operating systems. This will assist with the quality of the data held within these systems only being held, stored, and managed once.

The Trust is obliged to meet its legislative and regulatory requirements and will take actions as necessary to comply with the legal and professional obligations as set out in the Records Management Code of Practice for Health and Social Care 2016. It will take into account the following statutory regulations and standards:

- The Public Records Act 1958.
- The DPA18.
- The UK General Data Protection Regulation.
- The Freedom of Information Act 2000 with particular focus on the Lord Chancellor's Code of Practice on the Management of Records under Freedom of Information.
- The Environmental Information Regulations 2004.
- The Limitations Act 1980.
- The Common Law Duty of Confidentiality.
- The NHS Confidentiality Code of Practice.
- Care Quality Commission Declaration.
- Information Governance Toolkit requirements.
- NHS Litigation Authority Standards.

- British Standards ISO 27001 Information Security Management (was BS7799).
- ISO 17799 Information Technology – Security Techniques.
- BS 10008:2016 – Evidential Weight and Legal Admissibility of Electronic Information.
- Records Management Standard ISO 15489.

2.3. The Trust remains compliant with the Care Act 2014 that was brought into place following the Francis Inquiry. It is now a criminal offence to supply, publish or make available certain types of information that is either false or misleading, where that information is required to comply with statutory or other legal obligation.

2.4. The Trust is committed to ensuring that all relevant information is provided at the point of patient care. It is also committed to supporting the integration of health and adult social care jointly held care records.

2.5. To address training and education needs for staff relating to correct and timely data entry, and to ensure that there is adequate focus on data quality as well as supporting clinical areas. To ensure through awareness sessions that administrative staff are clear what their priorities are in regard to data quality and other tasks that they have to complete.

2.6. The Trust is further committed to improving the standards and quality of its information and records, whilst ensuring confidentiality and security is maintained. This is done by ensuring the quality of the information is of a high standard to adequately support the conduct of all Trust business including that of patient care.

2.6.1. The Trust Board has adopted this Information, Record Management and Data Quality Policy. It aims to deliver standardised ways of working and a number of organisational benefits:

- Clear standards to manage information and records.
- Improved structure and quality of the content of health and corporate records.
- Quality data for activity reporting.
- Improved control, access and security of information and records.
- Compliance with legislation and external monitoring body's standards.
- Reduction in duplication of information and records.
- Improve the physical and electronic storage of information.
- An informed, educated, and competent workforce.

- Improved use of staff time.

2.6.2. The information within a clinical record must be based upon professional consensus that reflects best clinical practice. This policy should assist and not hinder the process of writing, communicating, and retrieving clinical information. Structure and standards are essential to ensure data can be reliably stored, retrieved, reported upon, and shared.

2.6.3. Managing the way in which staff handle images and recordings must be standardised to ensure that confidentiality is maintained and that the Trust can meet its obligations abiding by legislation and respecting one another's privacy and dignity. The standard within this policy will also provide guidance and advice to patients and visitors with respect to taking images on personal devices.

3. Scope

3.1. The policy applies to all NHS records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector and public records, regardless of the media on which they are held. This also includes records of staff, complaints and business/corporate records and any other records held either electronically or in a paper format. This policy also applies to Adult Social Care records where they are integrated with NHS patient records.

3.2. A record is defined as 'information created, received, and maintained as evidence and information by an organisation or individual, in pursuance of legal obligations or in the transaction of business'. The DPA18 defines a health record as 'consisting 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'.

3.3. Examples of records and functional areas that should be managed using this policy [but not limited to]:

3.3.1. Function:

- Patient health records (electronic or paper based, including all specialties and GP records).
- Records of private patients seen on NHS premises.
- Emergency Department, birth, and all other registers.
- Theatre registers and minor operations registers.
- Administrative records including personnel, estates and financial records and notes associated with complaints handling.
- Clinical imaging reports, output, and images.
- Integrated health and social care records.

- Data processed for secondary use purposes (not used for direct patient care, such as data for service management, research or for supporting commissioning decisions).

3.3.2. Format:

- Photographs, slides, and other images.
- Microfilm.
- Audio and video tapes, cassettes, CD-ROM.
- Digital recording such as Attend Anywhere.
- Media such as MS Teams, Zoom, WhatsApp.
- Emails.
- Computerised records.
- Scanned records.
- Text messages and social media (outgoing and incoming) such as Twitter and Skype.
- Websites and intranet sites that provide key information to patients and staff.

3.4. This policy is applicable to all staff members of the Trust as every member of staff has a responsibility for recording either business or clinical activity in a consistent and accurate way to ensure effective recording and retrieval of information and records. The key components of effective information and records management are:

- Record creation.
- Record maintenance (including tracking).
- Access and disclosure.
- Closure and transfer.
- Appraisal.
- Archiving.
- Disposal.
- Disaster planning/business continuity.

3.5. The Trust recognises that increasingly, services are delivered on a multi-agency basis supported by shared information and record systems. The definition of what is considered to be a Trust clinical record is becoming increasingly complex with shared information systems, and the Trust is committed to working with partner agencies to ensure that responsibilities for control, access and disposal of records are properly discharged and that the appropriate information sharing protocols are in place and adhered to.

3.6. This policy also applies to photography and recordings and specifically recordings made:

- On healthcare premises within or outside of the UK (including Theatres) and/or,
- As part of the assessment, investigation or treatment of patients' conditions or illness and may include video links in Theatres, and/or,
- For purposes such as teaching, training or assessment or healthcare professionals and students, research, or other health related uses which are not designed to benefit the patient directly, described as 'secondary purposes'.

3.7. This policy outlines the responsibility of staff with regard to the quality of the information/data that they handle and the importance of accuracy and that getting it right first time saves time (GIRFT).

4. Definitions / Glossary

Archives – are non-current or closed records. These records may be in any format (for example, electronic or paper) and must be subject to robust controls to ensure that they remain accessible should they be required at a future date.

Convenience copy – A copy taken of a record that is to be used for a limited period and then destroyed. The master copy is retained.

CQC – Care Quality Commission are an external regulator who provide measures for organisations to comply with.

Business Continuity – The ability of an organisation to carry on functioning and delivering its critical services if usual processes are not available. This may be an outage of power and electronic systems are not available. At this point an alternative process must be put in place, usually paper-based that will be used to retrospectively enter the information once the systems are back up and running.

Declaration - the process of defining that a document's contents (and some of its metadata attributes) are frozen as it formally passes into corporate control and is thereby declared as a record. Indicates that a document is of corporate value.

Disaster recovery – The ability of an organisation to respond to a natural or manmade catastrophic event such that it can continue to function. Disaster recovery is a sub-set of business continuity that is primarily focussed on the IT aspects of the Organisation's infrastructure.

Documents - provide guidance and/or direction or render judgments which affect the quality of the products or services delivered; documents can be altered, revised, and require less stringent control than records. Documents precede records in the information life cycle: records are formed by declaration of documents.

DQ – Data Quality.

DQAG – the Data Quality Assurance Group, this group receives updates from Information Asset Owners on the quality of the data held within their information assets.

Health Record (Medical Record) – defined as anything that contains information in any media, which has been created or gathered as a result of any aspect of the work of healthcare employees, which supports patient care and includes agency/casual staff. The health record is the Trust's main acute record and is also referred to as hospital record, patient case note, patient record, or patient notes. Information held in the following systems (but not restricted to) will also be considered to be a part of the patient record:

- Patient Administration System.
- Maxims.
- Bluespier.
- WebPACS.
- Galaxy.
- Oceano.
- OPAS.
- Medisoft.
- NerveCentre.

This policy also applies to records created for staff who attend and have a consultation with or receive treatment within the Occupational Health department.

GIRFT – Get It Right First Time

Indexing – to provide each document with a unique name to allow users to search and find information quickly and easily

Information Asset – an information asset is a system that holds data, both demographic and activity. For the purposes of this policy these systems are the Trust's critical systems [but not limited to]:

- Patient Administration System:
  - Inpatient module.
  - Outpatient module.

  - Referrals Index.
  - Tracking module.
  - Booked Elective Admissions.
- Maxims.
- Oceano.
- Galaxy.
- Bluespier.
- Physical Health Record.
- E3 Maternity.
- Electronic Staff Record.
- eRostering.

IAO – Information Asset Owner, is an individual with responsibility for the data held within an information asset and ensuring that there are business continuity and disaster recovery plans in place.

IGG – Information Governance Group, a group that oversees and provides assurance to the Trust that information is being managed appropriately and escalation points are in place to raise concerns. Action plans are put in place and monitored by this group.

Metadata - data describing the management, context, content, and structure of records.

Mobile Devices - Mobile devices include- Smartphones, Tablets, Digital Camera, laptop. Recording software includes – Cam Scan, voice recorder, camera, Video recorder.

PAS – the Patient Administration System, a system that holds all the demographic and episodic information relating to patients who have been treated by the Trust.

Permanent records – Records that have archival value and will be retained for historical purposes after their retention period has expired.

Personal Identifiable Data (PID) – information that identifies individuals, name, date of birth, NHS number etc.

Recordings – refer to clinical imaging, photography, video, and voice recordings but excludes recordings of telephone conversations, pathology slides containing human tissue or CCTV recordings of public areas in hospitals. Photographs of slides may be made without consent for the purpose of care or treatment of a patient, or for secondary purposes, providing that images are anonymised or coded. Recordings also includes the use of mobile phones and other mobile devices. Recordings may be conventional (analogue) or digital and may be originals or copies.

Records - 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. A record is a document which has been declared as a formal record, constituted of both content and metadata.

SAR – Subject Access Request, this is where individuals make a request to see their information.

NCRS – National Care Records Service.

Temporary records – Records that may be destroyed after their retention period has expired.

SUS – Secondary User Service.

5. Ownership and Responsibilities

As records activity is undertaken throughout the organisation it is important to ensure that mechanisms are in place to enable the designated lead to exercise an appropriate level of management of this activity, even when there is no direct line of reporting. This may include cross-department records and information working groups or individual information and records champions, who may also be Information Asset Owners.

5.1. Role of the Chief Executive

The Chief Executive has overall responsibility for records, information, and data quality management in the Trust and for ensuring the Trust meets compliance requirements. The Chief Executive has a particular responsibility for ensuring that it corporately meets its legal responsibilities and for the adoption of internal and external governance requirements, this is delegated to the Chief Information Officer.

5.2. Role of the Chief Information Officer (CIO)

The Chief Information Officer has Executive responsibility ensuring that the Trust meets its legal responsibility for the management and quality of records and information. He/she is responsible for ensuring that the strategic plan for records management is adopted and properly implemented. The operational delivery and medium to long-term strategic planning of the health records service across the Trust is the responsibility of the Records Services, PAS and Data Quality Manager. The Records Services, PAS and Data Quality Manager reports directly to the Chief Information Officer.

5.3. Role of the Chief Medical Officer (CMO)

The CMO has operational responsibility for clinical record keeping standards for the consultant/doctor body of staff.

5.4. Caldicott Guardian

The Caldicott Guardian has responsibility for ensuring that each patient focussed system has appropriate controls to support patient confidentiality. He/she has particular responsibility for reflecting patients' and staff interests regarding the use of personal identifiable data. He/she is responsible for ensuring personal identifiable data is stored and shared in an appropriate and secure manner.

5.5. Role of the Chief Nurse

The Chief Nurse has operational responsibility for clinical record keeping standards for nurses, midwives, and allied health professionals.

5.6. Role of the Senior Information Risk Owner (SIRO)

The CMO is the Senior Information Risk Owner for the Trust. The role of SIRO is to own the organisation's information Risk Policy and to act as an advocate for information risk on the Board. The SIRO's responsibilities are:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers.
- Owning the organisation's overall information risk policy and risk assessment process and ensuring they are implemented consistently by Information Asset Owners (IAOs).
- Advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls.
- Owning the organisation's information incident management framework.

5.7. Role of the Records Services Manager

The Records Services Manager is responsible for the overall development and maintenance of information and record keeping policies, procedures, standards, and practices throughout the Trust, in particular drawing up guidance for robust records management, which includes corporate records and clinical record keeping standards, promoting compliance with policy, legislation and external standards. The Records Services Manager is responsible for the delivery of the operational health records service across the Trust and is specifically responsible for overall delivery of records management for Regulation 17 Good Governance, specifically 17(2)(c)(d) within the Care Quality Commission standards and particular standards within the Data Security Protection Toolkit and relevant NHSLA frameworks. The Records Services Managerwill work in close association with the Head of Information Governance (and Data Protection Officer for the Trust). The Records Services Manager will have an up-to-date knowledge of, or access to, expert advice on the laws and guidelines concerning confidentiality, data protection (including Subject Access Requests), and Freedom of Information requests.

5.8. Role of the Deputy Service Manager (Records Management)

The Trust's Deputy Service Manager (Records Management) holds day-to-day responsibility for delivery of corporate records management across the Trust. The Deputy Service Manager will advise on policy and best practice and is responsible for ensuring the creation and implementation of records management tools and guidelines and that records management systems and processes are developed, co-ordinated and monitored.

5.9. Role of the Head of Information Governance (Data Protection Officer)

The Head of Information Governance is also the Trust's Data Protection Officer and responsible for ensuring that the Trust is compliant with the DPA18, UK GDPR and the Freedom of Information Act 2000. There is a lot of overlap between managing information and the security of records and information, therefore the Head of Information Governance and Records Services Manager work closely together ensuring that information and records are being managed appropriately.

5.10. Role of the Operational Health Records Manager

The Trust's Operational Health Records Manager holds day-to-day responsibility for the operational delivery of the health records service and reports to the Records Services Manager. The Operational Health Record Manager will advise on policy and best practice and is responsible for ensuring that the policy and procedures are implemented and monitored, and that records management systems and processes are developed, co-ordinated and monitored.

5.11. Role of the Data Quality Team Leader

The Data Quality Team Leader ensures the Data Quality Team successfully deliver administrative support and data quality solutions to staff across the Cornwall Health Community in accordance with the agreed standards and within NHS policies and procedures. He/she ensures that system security is maintained at all times and that the teams' work is in accordance with the Data Protection Act 2018, Caldicott Report, IT Security Policy, and departmental procedures. The Team Leader must understand the impact upon legislation and Trust Policy and ensures software system security is maintained at all times and data is administered appropriately. The Data Quality Team Leader will ensure that errors are corrected in timely and appropriate manner. He/she will be responsible for highlighting areas of poor data quality to the Information Asset Owners and appropriate managers and provide recommendations to resolve issues in the future.

5.12. Role of the Information Services Manager

The Information Services Manager is responsible for highlighting areas of poor data quality in those systems that submit data to the Secondary User Service (SUS).

5.13. **Role of the Clinical Coding Manager**

The Clinical Coding Manager works closely with the Data Quality Team Leader identifying areas of poor data quality that need to be rectified to ensure accurate funding is recouped for the Trust.

5.14. **Role of the Information Asset Owners (IAO)**

The Information Asset Owners (IAOs) will support the Senior Information Risk Owner (SIRO) in their overall risk management function. Key responsibilities are to take ownership of the asset, review who has access to the information asset and to review and prioritise perceived risks and put in place actions to mitigate the risk. IAOs will respond to incidents or recover from a disaster affecting their information assets and ensure staff are aware of and comply with expected Information Governance working practices of the information asset. They will ensure that business continuity plans are available and tested. They will manage and control access to their systems ensuring appropriate training has taken place. IAOs are responsible for the quality of data held within their systems and completing the monthly dashboard to report improvements. IAO's are responsible for ensuring that reviews are conducted periodically on contracts relating to their systems, in conjunction with CITS.

5.15. **Role of Care Group Managers and Line Managers**

5.15.1. To ensure that staff have read and understood policies and procedures relating to managing records and quality of data entries within their areas/specialties.

5.15.2. Ensuring that departmental systems have up to date procedures available for staff which include procedures for the collection, validation, and entry of data (GIRFT).

5.15.3. Ensuring that any of their staff members involved with the capture, processing, storage and retrieval of audio, video and photographic recordings are aware of, and comply with, this policy.

5.15.4. To notify the Records Services Manager if recordings are undertaken in the department (not for each and every individual recording).

5.15.5. Supporting staff to ensure privacy and dignity is being maintained in the use of mobile devices in their departments/wards.

5.16. **Role of Care Group Governance Leads**

The responsibility for ensuring local record keeping practices are adopted and maintained is devolved to the Care Group Governance Leads. Care Group Governance Leads act as top layer. They have overall responsibility for the management of clinical/corporate/business records generated by their local business activities, i.e., for ensuring that records controlled within their departments/areas are managed in a way which meets the aims of the Trust's records management and data quality policies. They may decide to delegate this to a nominated member of staff.

5.17. **Role of the Community Records Managers**

The Trust holds clinical activity in the Cornwall Partnership Trust hospitals and other health facilities. The Community Health Records Managers will follow all RCHT policies, procedures, standards, and processes associated with records management, data quality and clinical record keeping standards and will ensure that they are implemented and monitored.

5.18. **Role of the Information Governance Group (IGG)**

The Information Governance Group is responsible for overseeing the Information Governance agenda and represents the interests of RCHT. It includes working with Responsible Authorities and other vested stakeholders in determining and ratifying Information Sharing Protocols, ensuring the best interests of RCHT patients and the functions of the business are served. It monitors progress towards the annual sign-off of RCHT Data Security and Protection Toolkit self-assessment obligations and receives and acts on breaches of confidentiality and information security. The Group is responsible for approving and ratifying appropriate policies, as well as identifying risks relating to its core business and ensuring that they are being managed appropriately. Information, data quality and records management forms part of its regular agenda.

5.19. **Role of the Data Quality Assurance Group (DQAG)**

The development, management and implementation of the data quality standards are the responsibility of the DQAG. This group is governed by the IGG and owned by CITS. The IGG agrees the Terms of Reference for this group to work within and accepts reports escalating concerns of poor data quality and actions to improve the quality of the data captured within the Trusts' many systems. This group is not currently running.

5.20. **Role of the Policy Review Group (PRG)**

The Policy Review Group is responsible for the final sign off for policies and guidelines to be uploaded onto the Trust's Document Library. They will apply and measure corporate standards against these documents before approval is agreed. Once agreed the Care Group Governance Lead will upload the document.

5.21. **Role of the Forms Review Group**

The Forms Review Group is responsible for applying the governance framework around all patient related paperwork and/or any output from an electronic patient system and agrees new and revised documents. Further guidance is available on the Forms Review Group website and Forms to Print webpage.

5.22. **Role of Individual Staff**

Most professionals working in health and social care have relevant codes of practice issued by their registration bodies and membership organisations of staff. Guidance is designed to protect against professional misconduct and to provide high quality care in line with professional bodies. The Academy of Medical Royal Colleges generic medical record keeping standards provide twelve individual criteria for staff when creating an entry into the patient record and this is discussed in more detail in Appendix 5.

5.22.1. All Trust staff, whether clinical or administrative, who create, receive, and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work and manage those records in keeping with this policy and with any guidance subsequently produced.

5.22.2. All staff who have responsibility for recording information must ensure that the quality of the information that they are recording is maintained using the standards detailed at Appendix 9.

5.22.3. Staff who collect and enter data have a responsibility to ensure its accuracy is validated and that any necessary corrections are made/reported promptly to the Data Quality Team.

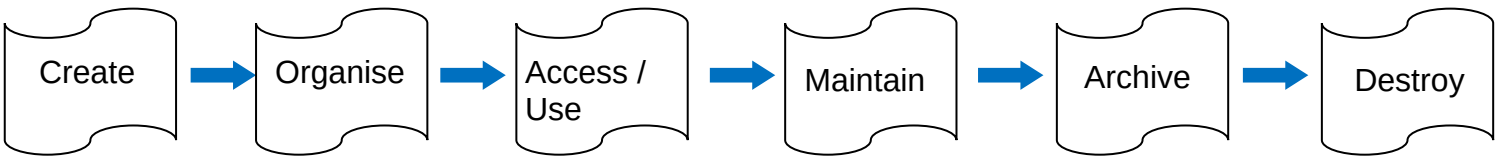
5.22.4. All Trust staff who create, manage and store records have a responsibility to add these records to the Information Asset Register. They must also inform their line manager and the Records Management Team of the activity within the department.

5.22.5. Medical staff are reminded that serious or persistent failure to follow the policy with specific reference to recordings which is based upon GMC guidance may put their registration at risk.

6. Common Standards and Practices

There are a number of standards for the differing disciplines within Information and Records Management, but equally there are a number of generic standard practices that can be applied.

The records lifecycle is a common standard and describes the framework in which information is managed from the point that it has been created to the point of archive or destruction. This is seen shown below in a diagram:



6.1. **Characteristics of an Authoritative Record**

Record Characteristic	How to Evidence
Authentic (Genuine)	➢ It is what it claims to be. ➢ It is created or sent by the person claiming to have created or sent it. ➢ To have been created or sent at the time claimed.
Reliable	➢ Full and accurate record of the transaction/activity or fact. ➢ Created close to the time of transaction/activity. ➢ Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction/activity.
Integrity (Truthful)	➢ Complete and unaltered. ➢ Protected against unauthorised alteration. ➢ Alterations made after creation can be identified as well as the persons making the changes.
Useable	➢ Located, retrieved, presented, and interpreted. ➢ The context can be established through links to other records in the transaction/activity.

6.2. **Document Classification**

All information possesses a security classification. The Cabinet Office Government Security Classifications May 2018 (enforced from April 2014) defines the protective marking scheme and describes how information assets are appropriately protected. It also details how organisations can meet the requirements of relevant legislation and any international obligations. This applies to all information that is collected, stored, processed, generated, shared, disclosed, and disposed of.

The NHS use a variation of this scheme based upon patient data being classed as ‘NHS Confidential’ having the equivalence of ‘Official’ under the 2014 scheme although a limited subset of information should be marked as ‘Official Sensitive’ where if lost or stolen there would be more damaging consequences.

6.3. **Declaring a Record**

Within any record keeping system there must be a method of deciding ‘what is a record?’ and ‘what needs to be kept?’ This is known as ‘declaring a record’ and can be declared at the point of creation or it can be declared at a later date. The declared record is then managed is such a way that it will be held in an accessible format until it is appraised for further value or destroyed, according to the retention policy in use. Declaration makes it easier to manage information in accordance with legislation and business needs. The DPA18 and FOIA2000 apply to all recorded information whether declared as a formal record or not.

Some activity will be predefined as a record that needs to be kept, such as a clinical record. Other records will need to fulfil criteria as being worth keeping, such as business documents or emails.

Once a record has been declared that record type must be entered into the Trust's Information Asset Register (IAR).

6.4. Quality of Information

All information held within the Trust's systems, paper and electronic must be fit for purpose. All staff must ensure that when entering information that it is timely and accurate and that any incorrect entries are identified and reported to enable timely corrections. Staff must be trained to Get it Right First Time (GIRFT) and that this then saves time.

6.5. Managing Electronic Records

Digital information must be stored in such a way that it can be recovered in an accessible format in addition to providing details about those who have accessed the record. It must continue to be available, as needed, despite advances in digital technology. Digital preservation ensures that digital information of continuing value remains accessible and useable, for example information recorded on an electronic patient record may need to be accessed in 100 years (with supporting audit trail to show lawful access and maintain authenticity). The authenticity of an electronic record is dependent upon a number of things not least that it has sufficient metadata to allow it to remain reliable, integral, and useable. It must be remembered that any links that are used must be kept up to date as the record then loses integrity once the links are broken and do not work. The same would apply to email messages relating to patient care, if they are not stored with the record relating to the transaction, it is not integral as there is no supporting information to give it context.

6.6. Metadata Standards

Metadata is key in making it easier to manage and find information, irrespective of whether it is in the form of webpages, paper files, electronic information, or databases. To be effective metadata needs to be structured and consistent across organisations.

6.7. Review for Continued Retention

The time periods documented in the separate retention schedules for Corporate and Health Records are minimum periods that records must be retained unless they have been identified for transfer to the Public Records Office (PRO). The Trust must have a process in place to request that records are retained for longer than the recommended time, including any temporary extensions to support litigation, public inquiries, on-going FOI, or SAR requests. The Trust can set local policies on retention time periods in relation to specific circumstances beyond those identified in the retention schedules, however where those records contain PID, any decision must comply with the DPA18 principles. If retention times, go beyond the periods laid out in the retention schedules decisions must be documented and authorised by the DPO and IGG.

6.8. Individual Policy Standards

6.8.1. Managing Corporate Information and Records – Appendix 3.

6.8.2. Managing Health Records – Appendix 4.

6.8.3. Managing Clinical Information – Appendix 5.

6.8.4. Managing Recordings and Photography – Appendix 6.

6.8.5. Access to and Disclosure of Personal Identifiable Data – Appendix 7.

6.8.6. Access to Electronic Systems – Appendix 8.

6.8.7. Data Quality – Appendix 9.

7. Dissemination and Implementation

7.1. This policy will be published on the Trust Document Library following authorisation through the IGG. and by the Policy Review Group. Immediately following publication, the Records Services Manager will ensure that its publication is highlighted across the Trust. Implementation of this policy will be supported through a series of briefings, departmental visits and training as required to highlight differences from the preceding policy and resolve records management and data quality issues as they arise.

7.2. This policy has been merged into one policy with standards appended, and replaces the following individual policies:

- Information Lifecycle and Corporate Records Management Policy.
- Managing Health Records Policy.
- Clinical Record Keeping Policy.
- Policy for Recordings and Photography.
- Data Quality Policy.

Previous versions of the policies above will be archived using the processes developed for the management of documents in the Document Library.

7.3. All staff whether clinical or administrative, must be appropriately trained so that they are fully aware of their personal responsibilities with regard to record keeping, data quality and record management, and that they are competent in carrying out their designated duties.

7.4. No patient or client records or systems should be handled or used until training has been completed.

7.5. All new staff members, and those returning to work after a period of absence, are required to attend the Trust Corporate Induction Programme which includes a session on Information Security and Records Management. Attendance at this session will enable staff to understand their responsibilities with respect to

records management, data quality, handling information, information security, and confidentiality.

7.6. All Trust staff will be made aware of their responsibilities for record keeping, data quality and record management through a variety of methods, including (but not limited to):

- Corporate Induction.
- Specific training:
  - Records Leads – on-line training.
  - Administrative staff – Case Note Management.
  - F1 and F2 Junior Doctors.
  - Therapists, Nurses, and Allied Healthcare professionals.
  - Clinical systems training.
  - Patient Administration Training.
- Records Management Website.
- For the Record Newsletter.
- Document Library.

7.6.1. **Corporate Induction**

All staff, new or returning to a new appointment after a period of absence are required to attend the Trust Corporate Induction Programme. Specifically, there is an allocated section on Confidentiality, Information Security and Records Management. By attending this Induction, staff will understand their most basic responsibilities in handling information, information security, confidentiality and record keeping.

7.6.2. **Mandatory Training**

There is a training and development programme for all staff who handle health records. Appropriate training must be provided for all users of the health records systems to meet local and national standards Case Note Management Training is mandatory for all administration staff and will be delivered by the Records Management Service. There is a requirement to have refresher training annually.

Patient Administration System training is mandatory for all administration staff and will be delivered by Cornwall IT Services. All staff will complete a competency test before a password is issued.

Health Records and related staff are encouraged to undertake the professional qualification awarded by the Institute of Health Records and Information Management, the Certificate of Technical Competence, although other qualifications may be available.

Health Records staff at supervisory and management level are encouraged to undertake the professional Health Records and Information Management qualification by examination, although other qualifications may be available.

Implementation of the classification of documents is dependent upon identifying document types and assigning a classification and updating the Trust's Retention and Destruction Schedule, as well as the Information Asset Register. Once this has been accomplished this will be cascaded through the Care Group Governance Leads and Senior Managers in the organisation.

7.6.3. Electronic Patient Systems

All staff are expected to complete on-line training or attend classroom training relating to specific systems before any passwords are issued. Requests for this training should be endorsed by the Line Manager and authorised by the Information Asset Owner which may be delegated to the IT Clinical and Business Teams.

Staff will be monitored with regard to incorrect information being recorded and will be sent letters informing them of the incident. This will be followed up on three occasions before passwords are removed and face to face classroom training and assessment is delivered. Passwords will be reinstated and should the member of staff continue to make errors a recommendation to their Line Manager will be made to consider their capability.

7.6.4. Records Management Website

The Trust's Records Management website, which is accessible on the Internet and Intranet, contains a wide range of information that has been derived from Trust policies, industry best-practice and regulatory standards. In addition to records management resources such as forms, procedures, presentations, FAQs, and guidelines the web pages contain information on the information lifecycle, a link to the Information Asset Register and links to external standards bodies.

The Records Management website is maintained by the Records Services Manager and the Deputy Service Manager (Records Management).

8. Monitoring compliance and effectiveness

8.1. The Trust may be asked for evidence to demonstrate that they operate a satisfactory records management regime. There are a range of sanctions where records management is found to not meet the required standard and sanctions previously made range from formal warnings, dismissal, and professional deregistration, CQC intervention and fines. A prison sentence also may be a possibility. Staff that are professionally registered may be asked to provide evidence of their professional work to support continued registration.

8.2. The Trust must at least once a year conduct an audit of its records to understand the extent of their records management responsibilities. This will involve identifying the different types of records and where they are being stored and ensuring that there are IAOs or Governance Leads overseeing the management of their records. This process should lead to identifying business critical records (Vital Records) and provide assurance that there are Business Continuity Plans in place with disaster recovery included. The Information Asset Register will hold this information and will provide reports on the Trust's records held within the organisation.

8.3. Monitoring compliance and effectiveness (table) for each standard area will be found at the corresponding appendices following the standards:

- Managing Corporate Information and Records – **Appendix 3.**
- Managing Health Records – **Appendix 4.**
- Managing Clinical Information – **Appendix 5.**
- Managing Recordings and Photography – **Appendix 6.**
- Access to and Disclosure of Personal Identifiable Data – **Appendix 7.**
- Access to Electronic Systems – **Appendix 8.**
- Data Quality – **Appendix 9.**

9. Updating and Review

9.1. This policy will be reviewed every three years by the Records Services Manager, the Deputy Service Manager (Records Management), the Operational Health Records Manager and Head of Information Governance or more frequently if there are changes to legislation, guidance, and best practice.

9.2. Any revision and update to this policy must be recorded in the Version Control table as part of the document control process.

10. Equality and Diversity

10.1. This document complies with the Royal Cornwall Hospitals NHS Trust service Equality and Diversity statement which can be found in the Equality Diversity And Inclusion Policy or the Equality and Diversity website.

10.2. Equality Impact Assessment

The Initial Equality Impact Assessment Screening Form is at Appendix 2.

Appendix 1. Governance Information

Information Category	Detailed Information
Document Title:	Management of Information, Records and Data Quality Policy V5.0
This document replaces (exact title of previous version):	Management of Information, Records and Data Quality Policy V4.0
Date Issued / Approved:	April 2024
Date Valid From:	May 2024
Date Valid To:	May 2027
Author / Owner:	Katie Day, Records Services Manager, Cornwall IT Services
Contact details:	01872 254500
Brief summary of contents:	This policy provides the framework within which the Trust will manage its corporate and health information and records, so they are controlled effectively, commensurate with legal, business, and operational information needs.
Suggested Keywords:	Policy, Policy Control, Procedural Documents, Procedures, Publishing, Publications, Photography, Corporate Governance, Corporate Identity, Corporate Image, Corporate Management, Corporate Records, Knowledge, Knowledge Management, Documents, Documentation, Records, Records Handling, Records Management, Records Retention, Records Disposal, Subject Access Request, Access Control, Recordings, Data Quality.
Target Audience:	**RCHT:** Yes **CFT:** No **CIOS ICB:** No
Executive Director responsible for Policy:	Chief Information Officer
Approval route for consultation and ratification:	Information Governance Group
Manager confirming approval processes:	Chief Information Officer

Information Category	Detailed Information
Name of Governance Lead confirming consultation and ratification:	Not applicable
Links to key external standards:	• CQC Regulation 17 Good Governance. • Data Security and Protection Toolkit. • Freedom of Information Act 2000. • The Public Records Act 1958. • DPA18 / UK GDPR. • The Freedom of Information Act 2000. • The Environmental Information Regulations 2004. • The Limitations Act 1980. • The Common Law Duty of Confidentiality. • The NHS Confidentiality Code of Practice. • Records Management Code of Practice for Health and Social Care 2021. • NHS Litigation Authority Standards Records. • Material published by the Professional Records Standards Body (PRSB) for Health and Social Care Standards.
Related Documents:	• Policy for the Development and Management of Knowledge, Procedural and Web Documents (Policy on Policies). • Records Management Strategy. • Corporate Records Management SOPs. • Information Security Strategy. • Information Use Framework Policy.
Training Need Identified:	Yes, for clinical administrative staff who handle patient records. Care Group Governance Leads to be made aware of policy and changes.
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Internet and Intranet
Document Library Folder/Sub Folder:	Health Informatics / Corporate and Health Records

Version Control Table

Date	Version Number	Summary of Changes	Changes Made by
13 October 2013	V1.0	Initial Issue – merging of the following policies: • Information Lifecycle and Corporate Records Management Policy. • Policy for Recordings and Photography. • Policy for Clinical Record Keeping. • Policy for Managing Health Records.	Kim Bellis, Records Services, PAS and Data Quality Manager
28 April 2014	V1.2	Added following policies: • Access to and Disclosure of Personal Information. • Access Control (Appropriate parts).	Kim Bellis, Records Services, PAS and Data Quality Manager
01 January 2015	V2.1	Opening times in WCH Library changed.	Not known.
14 March 2016	V2.2	Added a paragraph in Appendix 2 to cover the movement of patient records within the hospital.	Kim Bellis, Records Services, PAS and Data Quality Manager
4 January 2017	3.0	Full review and update in light of new Code of Practice issued by the Information Governance Alliance.	Kim Bellis, Records Services, PAS and Data Quality Manager
June to August 2017	3.0	Appendices sent to the appropriate owners to review and update.	Simon Thorogood, Mark Scallan and John Lewis / Jayne Martin.
October 2017	3.0	Minor amendments following review.	Kim Bellis, Records Services, PAS and Data Quality Manager
May - August 2018	3.1	Changes to reflect the change in legislation with the General Data Protection Regulations otherwise known as the DPA18 replacing the Data Protection Act 1998. Changes also to reflect transfer of service	Mark Scallan, Head of Information Governance Kim Bellis, Records

Date	Version Number	Summary of Changes	Changes Made by
		from CSCS Division to HI and ICT and therefore change in roles. Inclusion of statement regarding original records being sent to Derriford following a Coroner's Inquest recommendation.	Services, PAS and Data Quality Manager
May 2020 to April 2021	4.0	• Three-year review. • Move to new policy format. ➢ Information Governance Cover Sheet moved to Appendix 1. ➢ New EIA Cover sheet moves to Appendix 2. ➢ All subsequent appendices renumbered. • Inclusion and merge of Data Quality Policy into this policy. • Changing Divisions to Care Groups. • Inclusion of new Code of Practice from NHSX. • Change of Executive responsibilities. • Inclusion of images/recordings sent to the Trust from external sources. • Appendix 7 reviewed and further updated in line with GDPR and DPA 2018. Further minor changes throughout the document following review by IT Security IG manager.	Kim Bellis, Records Services, PAS and Data Quality Manager, and Mark Scallan, Head of Information Governance
April 2024	5.0	• Minor amendments following scheduled review. • Updates to links and references to the most recent policy versions. • Update to new Trust Policy format. • Updates to job titles.	Katie Day, Records Services Manager. Elise James, Deputy Service Manager. Kerensa Downing, Data Quality Team Leader. Mark Scallan, Head of Information Governance

All or part of this document can be released under the Freedom of Information Act 2000.

All Policies, Strategies and Operating Procedures, including Business Plans, are to be kept for the lifetime of the organisation plus 6 years.

This document is only valid on the day of printing.

Controlled Document.

This document has been created following the Royal Cornwall Hospitals NHS Trust The Policy on Policies (Development and Management of Knowledge Procedural and Web Documents Policy). It should not be altered in any way without the express permission of the author or their Line Manager.

Appendix 2. Equality Impact Assessment

Section 1: Equality Impact Assessment (EIA) Form

The EIA process allows the Trust to identify where a policy or service may have a negative impact on an individual or particular group of people.

For guidance, please refer to the Equality Impact Assessment Policy (available from the document library) or contact the Equality, Diversity, and Inclusion Team rcht.inclusion@nhs.net

Information Category	Detailed Information
Name of the strategy / policy / proposal / service function to be assessed:	Management of Information, Records and Data Quality Policy V5.0
Department and Service Area:	Records Management, Cornwall IT Services
Is this a new or existing document?	Existing
Name of individual completing EIA (Should be completed by an individual with a good understanding of the Service/Policy):	Katie Day, Records Services Manager
Contact details:	01872 254500

Information Category	Detailed Information
1. Policy Aim - Who is the Policy aimed at? (The Policy is the Strategy, Policy, Proposal or Service Change to be assessed)	The aim of this policy is to establish a consistent and coherent approach to handling corporate and clinical information and records, ensuring that the Trust meets its statutory and regulatory obligations.
2. Policy Objectives	The purpose of this policy is to establish a framework for the Trust in how it will manage its corporate and clinical information and records effectively and to ensure that procedures are in place for the creation and management of authentic, reliable, and useable records, capable of supporting business functions and activities for as long as they are required, in whatever format and media they are presented. This policy will underpin and support the delivery of the Digital Strategy.
3. Policy Intended Outcomes	Implementation of this policy will enable the Trust to achieve a high standard of information and records management leading to compliance with CQC Regulation 17 and IGT DSPT requirements. Business benefits include more efficient, safe patient care and a robust foundation for corporate decision making.

Information Category	Detailed Information
4. How will you measure each outcome?	Each standard has its own specific and targeted tools to measure their outcomes.
5. Who is intended to benefit from the policy?	The Trust and its partners, staff, patients, and the general public.
6a. Who did you consult with? (Please select Yes or No for each category)	• Workforce: Yes • Patients/ visitors: No • Local groups/ system partners: No • External organisations: No • Other: No
6b. Please list the individuals/groups who have been consulted about this policy.	**Please record specific names of individuals/ groups:** Head of Information Governance/Data Protection Officer. Information Governance Group.
6c. What was the outcome of the consultation?	Approved by IGG
6d. Have you used any of the following to assist your assessment?	**National or local statistics, audits, activity reports, process maps, complaints, staff, or patient surveys:** No

7. The Impact

Following consultation with key groups, has a negative impact been identified for any protected characteristic? Please note that a rationale is required for each one.

Where a negative impact is identified without rationale, the key groups will need to be consulted again.

Protected Characteristic	(Yes or No)	Rationale
Age	No	This policy addresses the management of information and records and takes into account the age of children's records and their respective mother's records when appraising for destruction, following Health and Social Care Information Centre guidance.
Sex (male or female)	No	This policy addresses the management of information and records and takes into account the fact that some females will have children, and this will have a bearing on the appraisal of retention and destruction of records, following Health and Social Care Information Centre guidance.

Protected Characteristic	(Yes or No)	Rationale
Gender reassignment (Transgender, non-binary, gender fluid etc.)	No	This policy advises on how to manage patients who are reassigned a new gender.
Race	No	This policy addresses the management of information and records, and this is not affected by Race/Ethnic communities/groups
Disability (e.g. physical or cognitive impairment, mental health, long term conditions etc.)	No	This policy addresses the management of information and records and is not affected by disabilities
Religion or belief	No	This policy addresses the management of information and records, and this is not affected by Religion or Other Beliefs
Marriage and civil partnership	No	This policy addresses the management of information and records, and this is not affected by marriage or civil partnerships
Pregnancy and maternity	No	This policy addresses the management of information and records and takes into account the fact that some females will have children, and this will have a bearing on the appraisal of retention and destruction of records, following Health and Social Care Information Centre guidance.
Sexual orientation (e.g. gay, straight, bisexual, lesbian etc.)	No	This policy addresses the management of information and records, and this is not affected by sexual orientation

A robust rationale must be in place for all protected characteristics. If a negative impact has been identified, please complete section 2. If no negative impact has been identified and if this is not a major service change, you can end the assessment here.

I am confident that section 2 of this EIA does not need completing as there are no highlighted risks of negative impact occurring because of this policy.

Name of person confirming result of initial impact assessment: Katie Day, Records Services Manager.

If a negative impact has been identified above OR this is a major service change, you will need to complete section 2 of the EIA form available here:
Section 2. Full Equality Analysis

Appendix 3. Corporate Information and Records Standards

1.1. Business Requirements

The key objectives of this policy are to ensure that:

- **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.
- **Staff members are trained** - So that all staff are made aware of their:
  - Responsibilities for record-keeping and record management.

1.2. Records and Information Lifecycle Management

Corporate Records Management is a discipline that utilises a system to direct and control the creation, version control, distribution, filing, retention, storage, archive, and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Trust. The key components of records management are detailed in the following sub paragraphs and more detailed instructions on the management of corporate records can be found in the Corporate Records Management Standard Operating Procedures (SOPs).

1.3. Creation, Capture and Maintenance

Creation

Staff should ensure that they create official records of all decisions and transactions made in the course of their official business. This can include making file notes of telephone conversations and minutes of meetings etc. Once created, all paper-based records should be placed on an official file which includes all official outgoing communications. Activities and business transacted electronically, including email, also need to be captured as part of a recordkeeping system. This will involve further work to be developed in ways of managing electronic records.

All records created by contractors performing work on behalf of the Trust belong to RCHT and are considered to be public records including the records of contract staff working on the premises as well as external service providers.

When creating a document, it is essential that a self-modifying file is not created, for example, the use of an automated date update must not be included in any document.

Capture

The Trust uses a web-based Information Asset Register through which all departments and areas should register the records that they are maintaining. The Information Asset Register is described in more detail in the 'Resources' section of this policy.

Maintenance

The maintenance and control of Trust records is documented in the Policy on Policies and is achieved as follows:

- **Trust-wide Procedural Documents.** Stored in the Document Library, subject to a strict review schedule and published under the control of the Policy Review Group.
- **Local Procedural Documents**. Stored on shared drives or network servers and managed by the appropriate departmental manager who assumes responsibility for the control and dissemination of the document as necessary.
- **Non-procedural Documents**. Stored on shared drives or network servers and managed by the appropriate departmental manager. If wider dissemination is required then non-procedural documents may be published on the relevant web page.

- **Web Documents**. Information contained within web pages may constitute a record and hence needs to be controlled. The authorisation of the relevant Service Manager must be obtained prior to publishing any document to either the Intranet or Internet.

1.4. Control, Tracking and Security

Control

RCHT must ensure that appropriate access and version controls are applied throughout records lifecycles, reflecting both legislative requirements and Trust policies. Where possible all staff must avoid duplication and printing copies of records. This increases risks of breaches of confidentiality and needlessly increases administrative costs borne by the Trust. When printed copies of records must be produced the copies must be destroyed as soon as the reason for their printing is finished. RCHT is committed to robust version control and consistent naming conventions applied to all corporate records and draft documents as detailed in the Corporate Records SOPs.

Tracking

This process enables retrieval of a record when required for correspondence or business and ensures that the current location of a file can be quickly verified. It is the responsibility of the individual sending a record to another person, department, or organisation to ensure that they obtain a receipt for the safe delivery of that record irrespective of whether the record is in hard copy or electronic. Similarly, when large quantities of records are transferred between departments, for example as a result of reorganisation, the department manager must inform the Deputy Service Manager (Records Management) so that the records can continue to be tracked.

Where records are held in long-term/archive storage areas it is essential that a record is kept of their movement to and from departments. The tracking flow and procedures for all archived corporate records will be managed by the Deputy Service Manager (Records Management).

There are certain record types that are particularly vulnerable and control/tracking systems are needed in place to ensure their security and long-term accessibility, for example, contracts.

Security

This section should be read in conjunction with the Trust policies listed as ‘Related Documents’ for a more detailed account of security, access, and disclosure arrangements. Records must be stored securely to prevent unauthorised access, destruction, alteration, or removal. All Trust staff members must take responsibility for the safe custody of all files and documents in their charge. Furthermore, records that are sensitive or hold confidential information must be placed in a secure storage area when not in use and must not be left unattended when in use. Manual or hard copy records must be stored in fireproof, damp proof, secure and preferably alarmed facilities with strict access controls in place. Trust records must be protected at all times from unauthorised disclosure, access, and corruption.

RCHT corporate/business records are not to be stored at home or left in cars unattended as they could be lost, damaged, stolen, or removed without consent. When a staff member temporarily leaves or resigns their post, they are required to leave all Trust records for their successors returned to the local filing system and be removed from all password protected systems. Please refer to the Leavers Checklist for Managers for further information on Trust requirements in this situation.

Authentication or Validation of Information

In cases where the authenticity of a record is in doubt the reader must refer to the owner, originator, or author of the document to check the record's veracity.

1.5. Access, Retrieval and Disclosure

Access.

Records must be available to all authorised staff members that require access to them for business purposes, when needed and in a timely manner. All access to RCHT corporate records by members of the public will be in accordance with the Freedom of Information Policy and records management procedures and access guidance.

Where corporate functions are outsourced contracts should clearly state that ownership of records resides with the Trust, and/or include specific instructions regarding creation, management, and access to the records created. The Corporate Records function should be consulted during the formulation of contracts where applicable.

Retrieval.

All Trust electronic corporate records should be stored on shared drives or servers as this enables efficient retrieval of information for staff in their daily work activities or processing of information access requests. This also ensures records are included as part of the corporate backups. Electronic messages and their attachments are subject to discovery during litigation, governmental investigations, and audits, and must be disclosed when responding to information access requests. To facilitate the retrieval and control of records an electronic corporate filing structure (Business Classification Scheme) will be introduced; refer to the 'Resources' section of this policy for more information.

Records must be stored in facilities where they can be identified, located, and retrieved; the retrieval and use of corporate records held in storage or offsite archive must be subject to controls in order to prevent damage and deterioration.

Disclosure.

Person identifiable information held in corporate records must be treated as strictly confidential and only be disclosed to individuals authorised in their day-to-day work to have access, or with the written consent of the person in question. Refer to the Trust's policy on Information Use Framework for more detailed information.

All requests for Trust information from the public, patients, external companies, or media must be channelled through the Freedom of Information procedures. Refer to the Information Use Framework Policy for further information or contact the Trust's Data Protection Officer. Any access requests for information that fall under the Environmental Information Regulations are currently channelled through the Freedom of Information Officer.

Particular consideration must be given to press releases to ensure that they do not contain any confidential information. The following requirements must be followed to ensure that Board level documents are not disclosed without due authorisation:

- All confidential Trust papers are to be printed on pink paper (including late additions).
- All Board packs are to be numbered and assigned to a Board Member.
- All Board packs are to be returned at the end of the Board meeting.
- Papers are to be made available for consultation and review via Share Point. Share Point is a secure system with individual controls and audit trails.
- Any papers sent via email must be either through 'nhs.net' accounts (not by Hotmail/Internet email accounts).
- Board room not to be left unattended, even during breaks.
- Access arrangements to secure drives used to store confidential papers is to be regularly reviewed (at least annually).

eDisclosure/eDiscovery and Records Implications

This is the disclosure of electronic records. In UK law, the civil procedure rules allow evidence to be prepared for court and as part of this, those involved in the litigation can agree what documents they disclose to the other party and dispute authenticity.

If records are arranged in an organised filing system, or all the relevant information is put into a patient/client file, this becomes easier to provide documents as evidence.

1.6. Appraisal, Retention and Disposal

Appraisal.

Where they have not been identified by the Records Management Code of Practice for Health and Social Care , Records Management function will appraise all record types to establish an appropriate management policy for that record type. Where appraisal decisions have been taken that amend, clarify, or otherwise affect the retention of records the retention schedule which can be found as a separate document on the Document Library will be updated. Once a record has reached the end of its retention period it must be handled as follows:

- Temporary records – destroyed in accordance with the retention schedule.

- Permanent records - stored in preparation for transfer to the Cornwall Record Office for permanent preservation.

- Convenience copies - destroyed without authorisation or recording at the discretion of the department who holds them once they are no longer required for the purpose for which they were produced.

There are three likely outcomes from appraising records:

1. Destroy or delete.

2. Keep for a longer period.

3. Transfer to the local Public Records Office.

Retention

It is a fundamental requirement that all RCHT's corporate/business records are retained for a minimum period of time for legal, operational, research and safety reasons. While the Trust has adopted the retention periods set out in the most recent NHS Code of Practice for Health and Social Care a retention and destruction schedule has been developed locally based upon the Code of Practice and provides a definitive reference for RCHT.

When e-mail is used as a transport mechanism for other record types, such as word processing documents or spreadsheets, it is possible, based on content, for the retention and disposition periods of the e-mail and the transport record(s) to differ. In this case, the longest retention period shall apply.

Disposal

After the retention period has passed and presuming there is no business need to retain the record for longer, all paper records due for destruction must be destroyed following the Trust's Waste Procedures for destroying confidential records. Destruction of electronic records follows the same standard as paper records. All Trust records held electronically, irrespective if created in digital form or scanned from paper copies, are covered by the same Retention and Destruction Schedule and their format makes no difference to their destruction requirements.

It is the responsibility of departmental managers to ensure that:

- The destruction of Trust records is recorded within the Information Asset Register

- Record retentions are reviewed at least annually.

- Records that have exceeded their retention period are disposed of in accordance with this policy. Disposal of mass volumes of paper records may require some additional requirements to safely dispose of and protect the security of records waiting collection.

All records classified as Permanent, thus requiring transfer to the local record office for permanent preservation, must follow Trust Transfer Procedures.

1.7. Storage/Archiving and Transfer

Storage/Archiving

Hardcopy records must be stored in appropriate storage areas that are safe, secure and protect the records from deterioration with appropriate access control measures applied to them. Rarely used or inactive records should be properly stored and maintained or transferred to offsite storage if space is limited. Requests for offsite storage can be directed to the Deputy Service Manager (Records Management). All archived records must be safeguarded against accidental loss, disclosure, or reconstruction wherever they are stored.

Records held in offices are generally those that are in current use with convenient storage areas utilised to store any archived records. These records must be securely stored to prevent theft or unauthorised access and their storage must conform to all current relevant legislation and guidance regarding Health and Safety. Where racking or shelving for storage is used it must be stable, of strong enough construction to support the weight of filled boxes, no more than 2.13 metres high from the floor. Wherever possible archived records should not be stored on shelves below knee level to minimise the risk of loss or damaged records in the event of flooding and assist Health and Safety lifting and moving aspects.

The Trust has a contract with external suppliers to provide secure storage for mainly non-current health records however, there is also limited space for corporate records. All corporate records stored offsite must still comply with retention periods and require controls to be introduced to ensure their appropriate management. To enable effective management of archived records all boxes holding archived, or semi active records, shall be appropriately labelled with information that lists content, department of origin, contact details, and retention period. A label template is available from the Records Management Website.

Transfer

Records of enduring value are transferred to the Cornwall Record Office's control and/or custody so that public archives are appropriately preserved. The Trust's Retention and Disposal Schedule indicates those records which are required to be kept as permanent archives. A Transfer Agreement between the RCHT, CFT and the Cornwall Record Office, has been signed at Chief Executive level detailing the responsibilities and obligations regarding the transfer of records to the public records office.

Guidance on the transfer process will be made available via the Trust's Records Management Website.

1.8. Transportation of Confidential Records

On occasion it may be necessary for a member of staff to carry confidential records. In such cases the following requirements must be met:

- The minimum number of confidential records should be transported.
    - This will be only for those meetings/commitments that occur during the same day.

- This should be limited to those meetings/commitments that are scheduled for the following day.

- Confidential records should only be left unattended for the minimum period.
- Confidential records should be transported in a secure bag.
- Records are locked in the boot of the vehicle and not visible in the main body of the car.
- At night confidential records should be securely stored within the premises of the member of staff transporting the notes. They should not be left anywhere that could be accessed inappropriately by non-trust staff.

1.9. Records Inventory (Information Asset Register)

Records Survey

Each department of the Trust is responsible for conducting a survey of their records holdings and recording the results of this survey in the Information Asset Register (IAR).

The IAR will benefit business processes by:

- Facilitating the classification and organisation of records.
- Recording the location of Trust records and who is responsible for them.
- Tracking disposal decisions whether by destruction or transfer.
- Improving the accessibility of records.
- Providing a critical analysis tool to measure and report on specific Trust record keeping habits.

The IAR can be accessed via the Records Management website on the Trust's Intranet with access to the application being via a password control administered by Cornwall IT Services (CITS). IAR entries must be maintained locally by the Service Manager with all entries being reviewed and updated at least annually. This will be monitored on a regular basis via Internal Audit and the Deputy Service Manager (Records Management).

1.10. Electronic records

The management of electronic records has been mentioned elsewhere in this policy however, as their management is notoriously problematic, it is worthwhile expanding on this issue further. To ensure that electronic records are managed appropriately all staff members must undertake conscious management at the earliest possible stage as this will determine the ultimate extent of control over electronic material. This includes, but is not limited to:

- Recording appropriate descriptive and technical metadata to provide sufficient contextual information throughout the life cycle of the record

- Maintaining records securely
- Ensuring that electronic records are protected during technological change
- Ensuring that record keeping procedures include data quality standards
- Ensuring that self-modifying files are not used, for example documents that contain an automatic date update

Maintenance and disposal of electronic records are determined by their content and must be in compliance with the retention schedule to this policy. Failure to properly maintain electronic records may expose the Trust and individuals to legal and operational risks.

As with paper records, electronic records must be protected from loss or deterioration however, particular threats to electronic records are accidental or deliberate erasure or alteration and the inability to access records due to changes in technology rendering the record file format obsolete. Assistance on solutions to these issues can be obtained from Cornwall IT Services (CITS).

To ensure that the Trust maintains access to the electronic records necessary to conduct its business CITS backs up servers to protect the information contained on all IT servers should loss or crash occur. Removable media (such as CDs, floppy disks, etc) may be used to make back-up copies of records; however, data contained on removable media still deteriorates over time. Therefore, removable media should only be used for short term storage and the Trust's servers should be used to store all electronic records.

Whenever new databases and automated systems are designed or purchased, records management should be consulted to determine early whether and what records should be created by the system. This may not always be necessary, but if not sure then staff should check with the Records Management function.

For existing electronic systems and databases, it is important to ensure that information is kept and remains accessible for as long as required. This may entail the migration of data when new systems are introduced.

Audio and Video Recordings

The Secretary and Chair of a meeting may decide to record the discussions of a meeting on audio tape, or other electronic means, instead of making handwritten notes (all meeting attendees should be made aware that a recording is being made). Where audio recordings are taken then these are to be treated in the same way as the handwritten notes that would otherwise have been produced, which means that once the contents of the tape have been transcribed into official minutes of the meeting, and the minutes have been approved by the Chair, the contents of the tape can be destroyed.

Destruction of audio and video tapes can be achieved by over-writing the contents of the tape as long as the recordings are not confidential. If the contents of the tape are confidential then the tape must be sent to Cornwall IT Services (CITS) for the attention of the IT Security Manager where it will be destroyed in accordance with CITS procedures.

1.11. Vital Records, Disaster Prevention and Recovery

Vital records are those records without which an organisation could not continue to operate. They are the records which contain information needed to re-establish the business of the organisation in the event of a disaster or significant interruption to

business, and which protect the key assets and interests of the organisation.

RCHT must protect these Vital Assets by managing them with strict controls that protect their existence and ability to access should there ever be the need. The Records Management Service, in collaboration with departmental managers, will:

- Identify critical processes, functions, and systems.
- Identify key internal and external dependencies on which these processes rely.
- Identify the records relating to the critical processes and functions.
- Make sure all departments identify, record, and protect their vital records.

Examples of records which might be classified as vital are:

- Minutes of management board meetings.
- Manuals and instructions.
- Pay rates and other personnel records.
- Annual reports.
- Legal documents, including current contracts.
- Computer software programmes and data.
- Accounts, payable and receivable.
- LDPs and formal Agreements.
- Communications/contact information.
- Indexes/finding aids to records.
- Policies and procedures.
- Building plans.

When vital records have been identified their existence must be recorded in the IAR and these records must then be appropriately protected to ensure that they are not lost or damaged. Vital records should be stored in protective or fire-resistant conditions with suitable access conditions; confidential records should be stored in locked storage cabinets. RCHT requires that disaster management programs are established and maintained to ensure that risks to records are managed appropriately.

Disaster recovery (business continuity) is concerned with ensuring that the Trust can continue to function in the event of a natural disaster such as catastrophic fire or flood or a man-made disaster such as hazardous material spills, infrastructure failure or acts of terrorism. Disaster recovery plans cover three main areas:

- Identification and protection of vital records.
- Measures to minimise the risk of occurrence of disastrous events.
- Recovery plans and procedures in the event of a disaster.

Each department of the Trust must produce a Disaster Recovery Plan that is reviewed at least annually to ensure that their vital records are adequately protected. Advice and assistance to generate a plan is available either through the Deputy Service Manager (Records Management) or via the Records Management Website.

1.12. Management of Specific Types of Corporate Records

Bring Your Own Device

Any record that is created for the use of health and social care business is the intellectual property of the employing organisation irrespective of it being created on personally owned computers and equipment. This also extends to emails sent from personal computers in the course of business. It is not permitted to store patient confidential information on any insecure device or system that does not meet the national requirements.

Complaints Files

It is necessary to keep a separate file where a patient complains about a service where there may be a subsequent investigation. However, this information must never be recorded in the patient's health record. Complaints may be unfounded or involve third parties and if this should be included in the patient's health record it will be preserved for the life of the record and may cause detrimental prejudice to any relationship between the healthcare professionals and the patient. Where multiple Teams/Services are involved in the complaint then all associated records must be amalgamated into one record, this ensures that everyone is aware of what is going on overall. Patients have a right to see a copy of their complaint file and if it is in one place it makes disclosure easier, also where complaints may be referred to the Ombudsman a single file is preferred.

Cloud Based Records

The NHS has a prohibition on storing patient identifiable data (PID) outside of England where there is a link to national systems or applications, so any solution must be able to trace servers back to England if it is going to be used for PID. Records in cloud storage must be managed as records in any other environment and the temptation to just increase storage space instead of managing records will not meet the recommendations in the Records Management Code of Practice.

There is a risk that Trust clinical or patient data could be lost or access to clinical patient administration systems, electronic health records or IT-based systems could be disrupted. This is caused by the increased potential for a cyber-attack or hack on the Trust IT infrastructure. This could lead to clinics or operations being cancelled, delayed, or significantly disrupted.

eDisclosure/eDiscovery and Records Implications

The relevant rule for disclosure and admissibility of evidence is given in the Ministry of Justices Civil Procedure Rules' Rules and Practices Directions as Rule 31.

If records are arranged an in organised filing system, such as a business classification scheme this process will be much easier to provide documents as evidence.

Email

This form of record is often neglected and therefore not managed well. Email has the benefit of fixing information in time and assigning the action to an individual, which are two of the most important characteristics of an authentic record. Emails are rarely saved in the business context, which is the third characteristic to achieving an authentic record. The correct place to save and store emails is in the file plan/record keeping system relevant to the business context and to declare the email as a record. The entire email must be kept, including attachments to the record remains integral, for example, an email approving a business case must be saved with the Business Case.

Automatic deletion of emails as a business rule may constitute an offence under Section 77 of the FOIA where it is subject to a request for information. A legal hold is placed on any information including email when an organisation enters into litigation; this means that they cannot be destroyed if there is a known process or an expectation that records will be needed for a future legal process. This means that no records can be destroyed by a purely automated process without some sort of review for continued retention or transfer to a place of deposit.

Emails that are the sole record of an event or issue, between a patient and clinician, should be copied into the relevant clinical record before being deleted.

It is good practice for staff to purge their email accounts upon transfer to another organisation to prevent a breach of confidentiality.

Funding

These types of records are primarily treated as administrative records but as they may contain large amounts of care information they must be managed as clinical records for their access and management.

Scanned Records.

Where information is scanned the main consideration is that the information can perform the same function as the paper counterpart did. Scanned records can be challenged in court. It is unlikely to be a problem provided that it can be demonstrated that the scan is an authentic record and that there are technical and organisational means to ensure the scanned documents maintain their integrity, authenticity, and usability as records through to appraisal and archive or destruction.

The legal admissibility of scanned records is determined by how it can be shown that it is an authentic record. The British Standard BSI 10008: 2016 - Evidential Weight and Legal Admissibility of Electronic Information specifies the method of

ensuring that electronic information remains authentic.

Wherever practicable paper copies of records should be scanned and retained electronically as this reduces the pressure on storage facilities and enables more efficient retrieval and dissemination of records. However, care must be taken when scanning large quantities of records to ensure that the scanned version is a true and accurate copy of the paper record. Therefore, a percentage of records must be quality assured to ensure that:

- Each document is legible.
- The documents haven't become skewed.
- That the records are complete, i.e. no pages are missing.

In addition, the paper record is to be retained for a period of three months following the production of the scanned record in case any instances of poor scanning are highlighted following the quality assurance checks detailed above. The storage of scanned records must also conform to the records management requirements applicable to all electronic records.

Social Media

If social media is used as a means of communication information for business purposes, then it may be a record that needs to be kept, and within the record keeping system. This may not necessarily mean that the social media must be captured but rather the information of the activity through transcription.

Staff Records

The content of a staff record should be sufficient for decisions to be made about employment matters. The essential paperwork will have been collected through the recruitment process, and will include:

- Job advert.
- Application form.
- Right to work.
- Identity checks.
- Correspondence relating to the acceptance of the contract.

It is usual for the Line Manager to hold the file, but this practice runs the risk of files being lost if there is an internal move of the member of staff. It is essential that all records are tracked when they are moved between departments, and hand delivered.

Upon termination of contract, records must be held up to and beyond their statutory retirement age. Records may be retained beyond 20 years if they continue to be required for NHS business purposed, in accordance with Retention Instrument 122. They are not exempt from Article 6(1)(e) of the DPA18 – Personal information must be kept in a form which permits identification of data subjects for no longer than is

necessary for the purposes for which the data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'). To reduce the burden of storage space it is recommended that a summary be prepared and held until the employee's 75th birthday or 6 years after leaving whichever is the longer and then reviewed. The summary must contain as a minimum:

- Summary of the employment history with dates.
- Pension information including eligibility.
- Work related injuries.
- Exposure to asbestos, radiation and other chemicals which may cause illness in later life.
- Professional training and professional qualifications related to the delivery of care.
- List of buildings where the member of staff worked and the dates in each location.

Disciplinary files should be held in a separate file so they can be expired at the appropriate time. That does not mean that there should be no record that the disciplinary process has been engaged in the main record.

Websites as Business Records

People's behaviour could be as a result of interacting with a website and it is considered to be part of the record of activity. For this reason, websites form part of the record keeping system and must be preserved.

1.13. Risk Management and the Assurance Framework

Procedures for risk assessment and the identification of vital records are the same for records in all media. The storage of records in electronic form may involve significant risks but many of these can be avoided by the use of adequate storage plans and strategies. A back-up system is generally recommended. All identified risks or incidents pertaining to the management of corporate records are to be recorded in the Trust's risk system DATIX; they are then managed via the Risk Process and Assurance Framework reporting.

1.14. Retention Schedule

Retention times in the schedule are those for operational purposes. Selection for transfer under the Public Records Act 1958 is a separate process designed to ensure the permanent preservation of a small core of key records which will:

- Enable the public to understand the working of the organisation and its impact upon the population it serves, and,

- Preserve the information and evidence likely to have long-term research value.

Selection of records for the Permanent Place of Deposit will be the responsibility of the Records Services Manager in conjunction with the Manager from the local Place of Deposit. If patient records are identified as of being of interest and the local Place of Deposit agrees then consultation will take place with the appropriate clinicians, Caldicott Guardian and Research Lead.

The retention periods listed in the retention schedule must always be considered minimum. It is legitimate to vary common practice where a well-reasoned case for doing so is made, recorded, and approved by the IGG.

1.15. Monitoring compliance and effectiveness

Compliance with this policy will ensure that the key aspects of CQC Essential Standard Regulation 17 – Good Governance (Managing Records and Information).

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	IAR use. Electronic filing systems. Disposal of records in accordance with the retention schedule. Maintenance of Business Continuity Plans. Maintenance of Vital Records
Lead	Deputy Service Manager (Records Management).
Tool	The Deputy Service Manager will conduct an audit with identified and agreed departments using a standard template with questions that will capture compliance with this policy.
Frequency	The Deputy Service Manager will conduct an audit annually of four areas.
Reporting arrangements	The audit report will be presented to the Information Governance Group and will align with the annual submission required for the Data Security and Protection Toolkit
Acting on recommendations and Lead(s)	The Deputy Service Manager (Records Management) will work with departments to undertake subsequent recommendations and action planning for any or all deficiencies. Required actions will be identified and completed within six months.

Information Category	Detail of process and methodology for monitoring compliance
Change in practice and lessons to be shared	Required changes to practice will be identified and actioned within six. months. A lead member of the team will be identified to take each change forward where appropriate. Lessons will be shared with all the relevant stakeholders through amendments to this policy, departmental presentations, and site visits.

Appendix 4. Managing Health Records Standards

Standards and Practice

Record Creation

The Trust/Cornwall IT Services will maintain the Patient Administration System, the electronic system through which patients are registered. Once a patient has been registered and allocated a unique NHS Number and a local hospital number, a health record can be raised. Please refer to the Health Records Case Note Management Mandatory Training material and the Health Records Standard Operating Procedure Manual for raising a case note folder.

The Trust is committed to using the NHS number to uniquely identify patients.

Electronic patient record systems should feed directly from the Patient Administration System, as the primary system, to ensure that the most up-to-date patient demographic information is being referenced. The Trust is committed to implementing a single electronic patient record.

Adopted Persons Health Records

Notwithstanding any other centrally issued guidance by the DoH or Department for Education, these records can only be placed under a new last name when an adoption order has been granted. However, before an adoption order has been granted an alias may be used. There may be in some circumstances situations where third party information needs to be protected, so additional checks must be mad before any disclosure of adoption documentation, because of the heightened risk of accidental disclosure. Any new records created for an adopted child must contain sufficient information to allow for continuity of care.

Ambulance Records

These records will contain evidence of clinical intervention and it is necessary to treat them as a clinical record. This information, whether stored as a separate record, or forming part of the hospital record must be retained for the same time as the clinical record.

Asylum Seeker Records

Records for asylum seekers must be treated in exactly the same way as other care records. Where the asylum seeker is given a patient held record the provider must satisfy themselves that they also have a record of what they have done in case of litigation or matters of professional conduct.

Continuing Care Decisions Records

Sometimes it is necessary for other organisations to access patient records when there are applications and/or appeals related to funding of continuing care. This sharing must be based upon consent and organisations should have arrangements in place to allow this. Any access must be lawful and the decision to grant access must be recorded.

Controlled Drugs Regime

Guidance and procedures have been established by NHS England with the NHS Business Services Authority and include information regarding storage, retention, and destruction. For further guidance refer to the most up to date NHS England guidance.

Family Records

These types of records were commonly seen within health visiting, some therapy services, and Clinical Genetics where a holistic picture of the family was needed to deliver care. This created an issue for the NHS and Social Care where records were attributed to individuals and managed as such. It is imperative that any disclosure of the individual's record is scrutinised to ensure that any third-party information is not disclosed without consent to do so. Due to changes in the law and best practice it is not advisable to create a single record containing information belonging to all the family. Good practice is to create a single record for each family member and refer to cross referencing of other family members.

Integrated Records

Issues of attributing ownership and access to integrated or joint records need to be resolved locally between all parties involved, identifying a lawful basis to access the record. Arrangements to consider:

- Nominating one organisation to own the records.
- Separating the records so that each party retains their own information.
- Each party keeps their own information but has access to the shared part of the other record.

For any of the options, patient consent will be necessary to allow all parties to access information lawfully.

The use of a Portal in effect creates a view into a number of systems relating to a patient and can then be used to inform decisions. The record is only correct at the time of viewing; therefore, it may be necessary to recreate the instance of viewing to allow an audit trail of decision making. This may be done by making a note in the record that the information has been obtained by this means to attribute the source of evidence for any interventions taken.

There are three types of retention for integrated records:

1. All organisations contribute to one record and the record is retained for the longest specialty period that was involved in the patient's care.
2. All organisations pool their records but keep a degree of separation between each type of record – refer to organisation's retention time periods.
3. All organisations keep their own information and allow others to view the record – refer to organisation's retention time periods.

Non-NHS Funded Patients Treated on NHS Premises

Where records of non-NHS funded patients are held in the record keeping system of the NHS or social care organisations, they must be kept for the same retention periods as other records outlined in the Code of Practice. They must be given the same levels of security and confidentiality.

Patient/Client Held Records

Where records are left with patients/clients it must be indicated on the record that they remain the property of the issuing organisation. Upon termination of treatment where the records are the sole evidence of the course of treatment and care, they must be recovered and given back to the issuing organisation. An example of this is a handheld maternity record.

Public Health Records

This function is usually hosted by a local authority and usually involves the handling of clinical information. It is expected that the standards will apply to the handling of confidential information will be those set in the Code of Practice for Confidential Information.

Records of Funding

These are primarily administrative records but do contain large amounts of care information and therefore must be managed as clinical records for their access management, based upon a lawful basis to share.

Sexually Transmitted Diseases Records

The NHS Trusts and Primary Care Trusts Directions 2000 impose an additional obligation of confidentiality on employees. This obligation prohibits some type of sharing but enables sharing where this supports treatment of patients. It is common for services dealing with sexually transmitted diseases to partition their records keeping systems to comply with the Directions and more generally to meet patient expectations that such records should be treated as particularly sensitive.

Specimens and Samples

The retention of these types of samples is not covered by this Code, but the metadata or information about the sample is. There is guidance issued by the relevant professional bodies on how long to keep human material.

Transgender Person’s Health Record

At the outset it is important to communicate with the patient as to their wishes on how they would like their records and information managed, based on explicit consent under common law. A patient can request that their gender be changed in a record by a statutory declaration, but it does not give them the same rights as those that can be made by the Gender Recognition Act 2004. At the time a GRA certificate is issued a new NHS number can be issued and a new record can be created, if this is what the patient wants. It is important that the patient understands the implications of not linking previous records with new records when they make this decision, as they may miss gender specific screening programmes.

Witness Protection Health Records

The right to anonymity extends to health records for those in the Witness Protection Scheme, and these records must be subject to greater security and confidentiality. These patients will be given new names and NHS number, so the records may appear to be that of a different person.

Record Keeping

Please refer to Appendix 5 for further information and help.

Record Maintenance:

Duplication and Version Control

There must only be one acute health record (physical or electronic) registered and raised for each patient, duplication of records puts patients and the organisation at risk. Where it is unavoidable and temporary folders have to be raised the key identifiable information must be available so that merging of the records as soon as is possible can take place safely and the tracking system updated to reflect the amalgamation.

Only a member of the Health Records Management Team may authorise a second folder to be raised once a full investigation has been conducted.

There may be occasion when two or more records on the Patient Administration System appear to be for the same patient. In this instance the Data Quality Team **must** be contacted. The Data Quality Team will determine if the records are for the same patients and will merge the records into one, ensuring that any other records in existence (both physical and electronic) for the patients are merged at the same time.

The Trust is committed to using the NHS number to uniquely identify patients.

Managing Records for Patients Changing their Identity

There are occasions when records can be changed, including, but not restricted to:

- Adoption.
- Gender Reassignment.
- Protection of Identity for individuals.

There are very clear procedures that must be followed in these cases; these changes are managed by the Data Quality Team.

Managing Records at Change of Contract

Once a contract comes to an end, the service provider still has a liability for the work they have done and as a general rule at any change of contract the records must be retained until the time period for liability has expired.

The standard NHS Contract documents that there is an option to allow the Commissioner to direct transfer of care records to the new provider to ensure continuity of care and service; this also includes third parties and those working under any qualified provider contracts. As the previous provider continues to have liability for their work there may be a need to make the records available for continuity of care or for professional conduct cases.

Where legislation creates or disbands public sector organisations, the legislation will normally specify which organisation holds liability for any action conducted by a former organisation. This may also be a consideration to identify the legal entity which must manage the records.

Where care records are being transferred to another organisation it may be necessary to inform the individuals of the change. If the impact is considered to be minimal then the use of posters and leaflets may be sufficient to inform people about the change. If, however, the change is significant then individuals should be communicated with and obtain explicit consent for the transfer of their record.

Examples of Managing Records at Contract change

Characteristic of New Service Provider	Fair Processing Required	What to transfer	Sensitive Records
NHS provider from the same premises and involving the same staff. This may be a merger or regional reconfiguration.	Light - appointment letter explaining that there is a new provider. Local publicity campaign such as signage or posters located on premises.	Entire record or summary of entire caseload.	Not applicable
Non-NHS provider from same premises and involving the same staff. This may be a merger or regional reconfiguration.	Light – notice on appointment letter explaining that there is a new provider. Local publicity campaign involving signage and poster and local communications or advertising.	Copy or summary of entire record of current caseload. Former provider retains the original record.	Not applicable
NHS provider from different premises but with the same staff.	Light – notice on appointment letter explaining that there is a new provider. Local publicity campaign involving signage and poster and local communications or advertising.	Copy or summary of entire record of current caseload. Former provider retains the original record.	Not applicable

Characteristic of New Service Provider	Fair Processing Required	What to transfer	Sensitive Records
NHS provider from different premises and different staff.	Moderate – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider.	Individual communications may not be possible so consent of current caseload may need to be sought before transfer. It may not be possible to transfer the record without explicit patient consent so in some cases no records will be transferred.
Non-NHS provider from different premises but with same staff.	Moderate – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider.	
Non-NHS from different premises and with different staff.	High – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider.	

Storage of records

Health Records Libraries

Health Records Libraries must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health and Safety at Work Act 1974 and Workplace (Health, Safety and Welfare) Regulations 1992. The Health Records Library at the Royal Cornwall Hospital holds records of patients who are currently being seen, there is also some secondary storage of records of patients who have not been seen recently. The Health Records Library at West Cornwall Hospital only holds records of patients who are currently being seen, all secondary storage of records are at the offsite storage facility.

Racking

Racking for storage is stable of strong enough construction to support the weight of health records and x-rays and is not more than 2.13 metres high from the floor. Racking must be metal and rolled edged.

Temperature

A reasonable temperature is maintained throughout the department between 15 to 19 degrees Celsius, where possible.

Ventilation

There is adequate ventilation in the department.

Lighting

There is adequate and appropriately sited lighting.

Annual Growth

Health records storage areas must be able to accommodate current needs and the annual growth of all health records.

Access

Access to the Health Records Libraries are restricted to authorised personnel only and must allow retrieval on a 24x7x365 arrangement.

Fire Safety

All fire exits must be clearly marked, and all staff must be up to date with their mandatory fire training. Fire-fighting equipment and alarms must comply with current standards and are inspected regularly. There are appropriately sited smoke alarms that are inspected regularly.

Equipment

There are adequate safety stepladders, safety stools and trolleys.

Filing

Health records will be filed in Terminal Digit order.

Security

Health Records Libraries should have a swipe card mechanism that only authorised personnel have access to. Access to the Health Records Libraries is controlled and authorised by the Health Records Management Team.

Offices

Offices must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health and Safety at Work Act 1974 and Workplace (Health, Safety and Welfare) Regulations 1992. Health records held in offices are generally those that are in current use either by the Clinician or Medical Secretary. Whilst the health records are in the offices they must be securely stored, filed alphabetically, and marked clearly if they are in particular clinic order, so that they are easily retrievable. Keys must be available through the Porters so that they are accessible out of normal office hours. All health records must be electronically tracked to the office.

Off Site Storage

The Trust has contracts with external companies providing secure storage for its non-current health records. The filing rooms at the off-site storage must conform to all the same relevant legislation as if they were filed on site at RCHT. Non-current health records are those that have not been seen between five and eight years, all records with the exception of the last year for deceased patients and temporary residents, it also includes children and maternity records, which are kept for twenty-six years. The Trust retains the function of destroying its records; this does not lie with the external contractor.

Racking

Racking for storage is stable of strong enough construction to support the weight of health records and x-rays and is not more than 2.13 metres high from the floor. Racking must be metal and rolled edged.

Temperature

A reasonable temperature is maintained throughout between 15 and 19 degrees Celsius, where possible.

Ventilation

There is adequate ventilation.

Lighting

There is adequate and appropriately sited lighting.

Annual Growth

Health records storage areas must be able to accommodate current needs and the annual growth of health records.

Access

Access to the health records filing rooms is restricted to authorised personnel only and must allow retrieval on a 24x7x365 arrangement

Fire Safety

All fire exits must be clearly marked, and all staff must be up to date with their mandatory fire training. Fire-fighting equipment and alarms must comply with current standards and are inspected regularly. There are appropriately sited smoke alarms that are inspected regularly.

Equipment

There are adequate safety stepladders and safety stools.

Filing

Health records will be filed in Terminal Digit order.

Security

Off-site storage should have an alarmed system linked to the local police station. Individual rooms storing health records will be securely padlocked and the key held within the Health Records Department only. Only authorised Health Records Staff will access these rooms at the off-site storage.

Wards

Whilst the health records are in use on the wards they must be securely stored, either in the secure lockable trollies provided to the Wards or in a locked office. Once patients have been discharged the health records should be moved to a secure office whilst summaries are dictated, and loose filing amalgamated within the records. The records must be filed in such a way and marked clearly so that they are easily retrievable at all times. All health records must be electronically tracked to the office. Whilst records and information are in use by individuals they must be removed from the nurses/ward clerk's station if they are called away or turned over so that the information cannot be read by unauthorised people.

Availability and accessibility of records

Health records should be available for every patient each time they attend hospital. All health records must be electronically tracked each time they are moved between locations, failure to do so may result in missing records. With the introduction of the electronic patient record, there will still be the need to use and track paper-based health records until such time as the electronic record is clinically rich and is recognised as the primary record. At a future point in time the need to use the paper record will reduce, with the expectation that paper records will become obsolete.

All staff are mandated to attend PAS Training. Administrative staff will specifically undertake the Tracking Module training before a password is issued.

Health records outside the Libraries are the responsibility of the individual that they are tracked to.

If health records cannot be located, then this must be logged with the Support Centre who will then inform the Records Management Team. An initial investigation will take place to locate the records and if at that point they are still missing then they can be added to front screen of the Patient Administration System. Missing records will be routinely looked for and if records are needed by the Legal Team a full and thorough investigation will commence with a fully documented audit of which areas have been looked in and how long the investigation has taken. Please refer to Operational Health Records Standard Operating Procedures for further information and instruction.

Requests for Health Records filed in the Libraries

The Health Records Library at the Royal Cornwall Hospital is open Monday to Friday between 07.00 and midnight, and between 09.00 and 17.00 Saturday and Sunday. All Bank Holidays are covered by staff working between 09.00 and 17.00, with the exception of Christmas Day when the Library is closed.

Health records retrieved out of normal office hours is by the Security Team. These health records will be tracked by administration staff working in the ED Department.

The Health Records Library at WCH is open Monday to Friday 09.00 – 17.00.

Requests for health records outside of these hours should be through the ED department at WCH. All Bank Holidays are covered by staff working between 09.00 and 17.00, with the exception of Christmas Day when the Library is closed.

Routine requests must be made using the Patient Administration System's spoolfile. Each request must contain enough information to be able to send them to the requester along with a date that they are required.

Urgent requests at RCH can be made by using the emergency telephone line 01872 254502 or by the fax 01872 254504.

Urgent requests at WCH can be made by using the telephone line 01736 874133. Requests made by email will not normally be accepted.

Transporting/Transmitting Health Records

Between Hospitals

All health records transported from one hospital to another must be in an orange bag or securely fastened in an envelope, and either moved by the Trust's approved Courier Service or with the contracted Taxi company. All vehicles used for transporting health records between hospitals should be:

- Either box-bodied or have a demountable container.
- In a suitable sealed container inside where a curtain side vehicle is used.
- Able to communicate with home base by radio or telephone.
- Fitted with electro-mechanical immobiliser or alarm system.
- Closed and locked/or sealed during transit.
- Immobilised or alarmed when left unattended.

The use of Trust vehicles on site that transport health records should be:

- Box bodied.
- Fitted with lockable and/or sealable doors.
- Able to communicate with the home base by radio or telephone.

- Attended to and not left unsupervised when records are on board.

All bags and envelopes must be clearly labelled with the destination, this helps to ensure health records do not go missing or end up in the wrong place.

Between Departments and Wards

All health records and loose documentation with personal identifiable information on them transported between departments and wards must either be in an orange bag securely fastened or in an envelope which is securely fastened. All bags and envelopes must be clearly labelled with the destination, this helps to ensure that health records do not go missing or end up in the wrong place.

Patients transporting their own health records

Patients who have appointments at two hospitals in the same day may be given their health records to bring with them to their next appointment, but they must be in a new envelope and sealed, it must then be signed by a member of staff across the seal then adhesive tape placed over the signature. Patients are not permitted to take their original health records home but may request copies of part of or the full health record under the DP18. See Appendix 7 Access to and Disclosure of Personal Identifiable Data (PID).

Security of health records in transit by Healthcare Professionals

The minimum of case notes should be transported and will be only for those consultations that occur during the same day and will be limited to those consultations that are scheduled for the following day.

Case notes should only be left unattended for the minimum period, (during consultations).

Case notes should be transported in a secure bag and locked in the boot of the vehicle and not in the main body of the car.

At night case notes should be securely stored within the premises of the member of staff transporting the notes. They should not be left anywhere that could be accessed inappropriately by non-trust staff.

All staff have a responsibility to report records left unattended by using the Trust's Datix reporting system.

Out of County

The original health record must not, under any circumstances, be sent out of the County. If you require further guidance on this contact either the Records Services Manager or the Head of Compliance (Data Protection Officer).

However, original patient records may be sent to Derriford Hospital, but they must be tracked with a contact telephone number and the Health Records Supervisor must be notified of this this. The Health Records Supervisor will check this list monthly to ensure that the records have been returned to the Trust.

Copies of health records

Copies of health records sent must securely, this could be through Kiteworks, secure email, encrypted disc, IEP or by Special Delivery. This is managed by the Disclosure Office. Copies of records must be legible and reflect the original record. Please refer to Appendix 7 Access to and Disclosure of Personal Identifiable Data (PID).

Electronically Transmitting information

The Trust recognises that part of the drive towards seamless care requires the sharing of information in order to improve the speed and efficiency with which health, education and social care organisations discharge their responsibilities. With all these changes taking place in delivering patient care, the way in which we communicate must be a key factor in these changes. The Trust has agreed that NHS professionals should be able to email patient information as an interim solution until such time as clinical messaging is embedded into our clinical systems. Please reference the Policy which can be accessed on the Trust's Document Library.

The Trust is moving toward the use of eFaxes and is removing the conventional faxes from use when they are due to be replaced. Where conventional faxes are still in place and being used, they must be located in a Safe Haven.

Scanning health records

The Trust is embarking on implementing a scanning solution for its patients who are currently being treated within the organisation. The Trust will ensure that the suppliers who are providing this solution are BS10008:2016 compliant and meet all the statutory, legislative, and best practice guidance. The Health Records Service will ensure that records sent off to be scanned will be managed in a documented and structured manner, all of which is detailed in the departmental Standard Operating Procedures.

Use of mobile devices to transport/transmit information

Please reference the Mobile IT Security Policy and Appendix 6, Recordings and Photography Standards.

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. The Trust must be able to form a reconstruction of activities or events that have taken place. There must be a full audit trail of all activity taking place within an electronic record. For further guidance please reference Appendix 5 Clinical Record Keeping Standards.

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.

Written Content

Health records serve many purposes; the most important is the contemporaneous record of events and assessments that assist diagnosis and treatment. It is important for these records to contain all relevant information about the patients so that any health professional can continue the care of the patient. For more detailed information on what is expected when recording information in the health record please refer to Appendix 5, the Clinical Record Keeping Standards.

Clinical Document Management

Refer to Appendix 5, Clinical Record Keeping Standards.

Appraisal, Archiving, Disposal, Closure and Transfer

Records can be maintained appropriately 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.

It is a fundamental requirement that all of the Trust's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record.

The Trust has adopted the retention periods set out in the Department of Health (DoH) Records Management Code of Practice: A guide to the management of health and care records. A retention and destruction schedule has been developed locally, based upon the Code of Practice, and provides a definitive reference for the Trust. The schedule will be reviewed regularly to reflect the most recent retention decisions. Any deviation from the DoH recommendations must be presented to the Information Governance Group for approval to become a locally agreed retention time period. *This document is available on the Records Management Website.*

Before any records are destroyed it must be established that there are no ongoing public enquiries that prevent destruction of records that may be needed.

Records identified for destruction must be destroyed in a confidential manner. The Health Records staff will carry out the appraisal of the main health record for either retention or destruction. These staff will be appropriately trained. The Health Records Service has a contract with an external local contractor to destroy its records by shredding and pulping. This should be to the BSIA Information Destruction Guide EN15713:2009.

Different formats of confidential records are categorised so that it is clear to what standard the information should be destroyed. The tables below describe the method of destruction:

Table 1.

Category	Description
A	Paper, plans, documents, and drawings
B	Negatives
C	Video/audio tapes, diskettes, cassettes, and film
D	Computers and any other computer related equipment such as hard drives, embedded software, chip card readers, components and other hardware, CDs, DVDs, and SIM cards. See Acceptable Use/IT Security Policy for further guidance.
E	ID cards
F	Counterfeit good, printing plates, microfiche, credit and store cards and other products
G	Corporate or branded clothing and uniforms
H	Medical x-rays and overhead projector slides
NOTE: Hazardous waste is not included in this table	

Table 2

No.	Average Surface area of material	Maximum Cutting Width	Method of destruction	Material Categories Acceptable/Unsuitable for material							
	mm2	mm		A	B	C	D	E	F	G	H
1.	5000	25	Shred	Yes	No	Yes	Contact CITS 1717	ID returned to Line Manager	Contact Records Management	Contact Linen Services	Yes
2.	3600	60	Shred	Yes	No	Yes					Yes
3.	2800	16	Shred	Yes	No	Yes					Yes
4.	2000	12	Shred	Yes	No	Yes					Yes
5.	800	6	Shred or disintegrate	Yes	No	NA					NA
6.	320	4	Shred or disintegrate	Yes	No	NA					NA
7.	30	2	Disintegrate	NA	Yes	NA					NA

No.	Average Surface area of material	Maximum Cutting Width	Method of destruction	Material Categories Acceptable/Unsuitable for material							
	mm2	mm		A	B	C	D	E	F	G	H
8.	10	0.8	Disintegrate	NA	Yes	NA					NA

Further guidance is available for staff on identifying records for retention/destruction in the Operational Health Records Standard Operating Procedures, available on the Records Management Website and the Document Library.

There must be a record of all patient records that have been appraised and either archived, scanned, or destroyed. Care needs to be taken when 'deleting' electronic records as this may be reversed and may not meet the standard as information can/may be retrieved. The ICO is clear with 'legacy systems' that as long as the information is beyond the reach of everyday staff then this will fulfil the criteria.

Records are secure

This section should be read in conjunction with the RCHT IT Security Policy and Acceptable Use Policy for a more detailed account of security, access, and disclosure. Both these polices can be accessed on the Trust's Document Library.

All new staff must attend the Staff Induction Programme where Confidentiality, Information Security and Records Management are presented.

All staff must understand their individual responsibility for the security of their workplace and records/information held there.

Manual records must normally be stored in fireproof, damp proof, secure and alarmed facilities with strict access controls in place, if this is not possible a risk assessment must be carried out to identify and record the risks and put measures in place to mitigate those risks.

Electronic records must be protected at all times from unauthorised disclosure, access and corruption and must be regularly backed up and stored off site. computer screens must be placed out of sight of the general public to protect information and must be turned off when unattended.

Personal information held on patients/clients is strictly confidential and must only be disclosed to individuals authorised, and have a legitimate relationship in their day-to-day work, or with the written consent of the patient/client (for further information please refer to Appendix 7, Access to and Disclosure of Personal Identifiable Data (PID). There are exceptions where disclosure is permitted, for example where under common law there is an overriding public interest or the investigation of a serious offence. The Data Protection Officer will be able to offer further advice.

Health Records in use must not be left unattended; this may lead to an unauthorised disclosure of information and breach of confidentiality.

Multiple records must be transported, dispatched, or posted internally using orange bags. Single records may be transported using clearly labeled envelopes securely sealed. Records sent externally and not by the Trust vehicles must be sent by Special Delivery.

There are procedures are in place to report and locate missing records. Please refer to the Operational Health Records Standard Operating Procedures.

Original health records should not be sent out of the County or taken home unless there are exceptional circumstances. If this becomes a necessity the Medical Director, Data Protection Officer or the Records Services, PAS and Data Quality Manager (with delegated authority) must be contacted prior to the records being sent/taken. In any event the records must be tracked on the Patient Administration system.

Working from home accessing electronic clinical information must be through Trust provided devices which will securely connect to clinical systems using Microsoft Direct Access and the appropriate procedures followed. Refer to the Working at Home Policy on the Trust's intranet.

Care that uunauthorised or inadvertent alteration or erasure in the record must be maintained. Access and disclosure must be properly controlled, and audit trails are to be in place to track all use and changes. Records must be held in a robust format, which remains readable for as long as they are required.

Content of records are secure

It is **every employee's responsibility** when handling the health record to ensure all documentation is securely filed and fastened within before it is returned to either the Clinical Coding department, the Health Records Department for filing or for onward transmission to another user/department. All documentation filed in the health record must be in accordance with the order of filing in the back of the health record folder. Means of securing documentation may vary in the health record, but adhesive tape or staples **must not** be used. Any loose filing must be securely filed and unable to be lost during transportation between departments etc. Complaints and litigation documentation **must not** be filed in the health record. Please refer to the Health Records Case Note Management Mandatory Training material for further guidance.

Where incorrect filing has been identified within a patient record it must be recorded using the Trust's Incident Reporting System, Datix, including as much information about the wrong information, who it belongs to and whose records it was found in. Do not remove the information. The Records Management Team/Data Quality Team will manage this through Datix. Where incorrect information has been identified in the electronic patient records this will be notified to the Data Quality Team through the appropriate method for that system.

Where personal identifiable information has been found in inappropriate areas it must be handed into the nearest Reception Desk and reported using the Trust's Incident Reporting System, Datix. The Records Management Team/Information Governance Team will manage this through Datix and will collect the identified information.

Risk Management, Disaster Planning and Business Continuity

Regular risk assessments are undertaken in line with the Trust's Risk Management Strategy. All risks will be recorded on the Trust's Datix Risk Management module and reviewed in a timely manner. All incidents reported relating to Records Management through the Trusts' Datix Incident Reporting module will be responded to in a timely manner and discussed and monitored at the CITS Quality and Risk Group (QARG).

Health Records are considered to be vital records, by the very nature that they are needed to treat the patient. These records must be managed in such a way to protect their existence. Please refer to the Health Records Business Continuity Plan held within the Department.

All health records must be kept in storage facilities and managed in ways that conform to Health and Safety and Fire Regulations to minimise the risk of permanent destruction by either fire, water etc.

In the event of a failure of the Patient Administration system please refer to the Business Continuity Plan, Health Records Policies and Departmental Standard Operating Procedures for instructions.

Cornwall IT Services ensures that clinical information on electronic systems is backed up on its servers.

Electronically held information must either be able to be migrated to new systems as they are introduced, if appropriate, or still accessible for the retention period if deemed inappropriate to migrate

Access and Disclosure of Records

Please refer to Appendix 7. Access to and Disclosure of Personal Identifiable Data (PID).

Retention Schedule

Retention times in the schedule are those for operational purposes. Selection for transfer under the Public Records Act 1958 is a separate process designed to ensure the permanent preservation of a small core of key records which will:

- Enable the public to understand the working of the organisation and its impact upon the population it serves and,

- Preserve the information and evidence likely to have long-term research value.

Selection of records for the Permanent Place of Deposit will be the responsibility of the Records Services PAS and Data Quality Manager in conjunction with the Manager from the local Place of Deposit. If patient records are identified as of being of interest and the local Place of Deposit agrees then consultation will take place with the appropriate clinicians, Caldicott Guardian and Research Lead.

The retention periods listed in the retention schedule must always be considered minimum. It is legitimate to vary common practice where a well-reasoned case for doing so is made, recorded, and approved by the IGG.

Monitoring compliance and effectiveness

Overall good records management ensures health records are available to provide evidence of any decisions made or reconsidered at a later date, and it is clear what has been done, or not done, and why. This is of vital importance in providing quality patient care, and also in cases of clinical liability.

Audit plays a vital role in ensuring that this policy is being implemented effectively to improve the quality of the health record service and in turn raise the standard of patient care. Furthermore, audit reports provide evidence to the regulatory authorities that the Trust is performing to the standard expected. Just as importantly audit provides independent verification to local management of the performance of their area and can suggest changes to working practices in order to improve service levels or adopt best practice. Audit should form part of the overall records management programme.

Any incidence of non-compliance with Trust policy will be included in an action plan for resolution.

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	1. Health Records Libraries: a. Health records retrieved. b. Health records filed. c. Internal movement of health records between filing sites. d. Number of temporary folders filed and amalgamated. e. Number of health records destroyed. f. Number of urgent requests received. g. Number of health records re-foldered. h. Number of loose documents filed. i. Number of Therapy records amalgamated into the main record. 2. Clinic Preparation: a. Number of health records required for clinic. b. Number of main health records requested and sent for clinic. c. Number of temporary folders sent to clinic. d. Number of referral letters missing. e. Number of health records re-foldered. f. Number of health records moved from old style to new style folders. 3. Management Team Activity: a. Unauthorised access to the Patient Administration System. b. Number and nature of informal complaints.

Information Category	Detail of process and methodology for monitoring compliance
	c. Number and nature of formal complaints. d. Number and nature of PAL's enquiries. e. Number of alerts recorded. f. Availability of notes at the start and end of the clinic (from within the outpatient departments). g. Clinical Record Keeping Audit – content of the record. Security of notes across the Trust – physical visit and complete proforma.
Lead	Records Management Team
Tool	**Methodology** A template is prepared with dates set for the Health Records Service to monitor activity once a month for one week. This template is available on the Departmental Shared Drive accessed by the Supervisors and Team Leaders. The Health Records Manager (Operational) collates all the information and produces graphical charts to be inserted into the report for the Information Governance Group. Information collected through the Reception and Ward Clerk staff is by completing a proforma, partially completed by Health Records staff before being sent out with the patient's health records. This information is returned to the Department Administrator within the Health Records Service and collated into a spreadsheet available on the Departmental Shared Drive. This is then used by the Health Records Manager (Operational) and included in the report. The audit report against the Patient Administration System is the responsibility of the Health Records Manager (Scanning) carried out every Friday morning and a printout is kept in the Records Management Service. This is then collated by the Records Services Manager and included in the report. Missing health records are managed and monitored through the Patient Administration System. The missing notes screen is printed on a weekly basis and filed within the Records Management Service. The Health Records Manager (Scanning) periodically goes through the list to see what records have been found and any that have been missing for a month or more instigates an in-depth search.
Frequency	Monitoring of activity is collected one week in four, and a different week in each month. The results are reported quarterly.
Reporting arrangements	**Information Governance Group (IGG)** The Records Services Manager will present reports to the IGG.

Information Category	Detail of process and methodology for monitoring compliance
Acting on recommendations and Lead(s)	The Records Services Manager will undertake subsequent recommendations and action planning for any or all deficiencies and recommendations within reasonable timeframes. The subsequent action plan will identify the recommendation and a specified timeframe for implementation.
Change in practice and lessons to be shared	Any system or process changes or lessons learnt will be shared with the Information Governance Group. This will also be shared through the Daily Bulletin and For the Record publication. Following any change, the Records Services, PAS and Data Quality Manager will arrange to re-audit.

Objectives

1. To provide evidence that this policy has been embedded throughout the organisation.
2. To provide evidence of compliance with this policy.
3. Monitor activity and Improve the quality of the health record service.
4. To improve the standard of patient care through improved record availability.
5. To assure information security is in place.
6. Provides evidence of performance in specialty areas.
7. To identify areas of improvement and document in an action plan.

Resources

These audits are reliant upon a number of staff groups:

- Health Records operational staff to collect information.
- Health Records Supervisors and Team Leaders to aggregate figures.
- Health Records Manager (Operational) to compile graphical report.
- Records Services Manager to finalise report and provide management section. Provides report on physical visits to departments/wards.
- Reception staff to complete monitoring of health records at start and end clinics.
- Ward Clerks to complete monitoring of urgent health records received.

External Monitoring Bodies

The following bodies are likely to want to see the results of these audits as part of the external monitoring process:

- Data Security and Protection Toolkit.
- Care Quality Commission.

Appendix 5. Clinical Record Keeping Standards

Structure of the Record

Throughout this section detailed information on each section can be accessed in the Health Records Service Standard Operating Procedures and Case Note Management Training material.

Record Creation

Front cover

The front cover of the record will display the following information:

- NHS Number.
- CR Number.
- Surname and Forename.

ALL PRINTED WITH BLACK MARKER PEN

- Patient ID Label containing the following:
  - NHS Number.
  - Surname..
  - Forename
  - Address.
  - Date of Birth.
  - CR Number.
- Bar code label (where appropriate).
- Year label.
- Alert label if appropriate.
- Any agreed Disability Awareness labels.
- Volume number of case notes.
- Identification of where case notes should be returned to for filing.

You must not record any clinical information on the front of the cover – this is a breach of patient confidentiality.

You must not use staples to affix anything to the front cover.

Inside Front Cover

General information is available on:

- Responsibility of filing.
- Entries must be legible and dated.
- Mandatory training.
- Creation and amendment of clinical documents.

Alerts and allergies must be recorded on the inside front cover. If a patient is known **not to have any allergies** this must be positively recorded.

All infection risks must be recorded and where appropriate the use of issued labels is encouraged.

The Records Management Service Team manages the following alerts centrally [not an exhaustive list], and updates the physical record and/or the Patient Administration System:

1. Acknowledgement of Responsibilities Agreement (ARA).
2. Clinically Related Challenging Behaviour (CRCB).
3. Children in Care (CIC).
4. Children on a child protection plan (CP).
5. Domestic Abuse.
6. General Safeguarding alerts.
7. Sealed information alerts.
8. Medication alerts.
9. Parkinson’s disease.
10. Lasting/Enduring Power of Attorney.
11. Managing children’s information where parents have separated.
12. Patients with similar names.
13. Living Wills/Advanced Directives.
14. Home Ventilation.

The Operational Health Records Service in conjunction with Microbiology and the Research Department manages the following alerts, and updates the physical record and/or the Patient Administration System:

15. MRSA (in conjunction with Microbiology).

16. ESBL (in conjunction with Microbiology).
17. HEP C (in conjunction with Microbiology).
18. PPD Mantoux Skin Testing (PPD Allergy – Mantoux).
19. Patients participating in research/trials.
20. Retention and destruction alerts.

To assure full compliance with our legal duties and to enable full disclosure of all records relating to a patient you must complete the table ‘Details of other records being held away from this file’. For example, records held on electronic systems such as (but not limited to):

- Bluespier.
- Maxims Clinical.
- Medical Photography.
- Therapies.
- Oncology.

Details of retention and destruction dates are completed by authorised staff within the Operational Health Records Service.

Inside Back Cover

The inside back cover of the case notes details the content structure of the health record and must be adhered to.

First Spine

Treatment Escalation Plan (TEP) (Allow Natural Death (AND))

The TEP has replaced what was the Allow Natural Death documentation. If the patient has completed a TEP form this must be filed in front of the Identification Sheet whilst it remains active. If this should become inactive it should be removed and filed in the Legal Section on the second spine. An orange alert sticker must affixed to the front cover of the record drawing attention to this.

Advanced Decisions (Living Wills)

Following the introduction of the Mental Capacity Act patients are more proactive in providing Advanced Decisions describing their wishes and intentions should they attend hospital and not be able to communicate this. These documents are to be filed at the front of the record behind the TEP form but in front of the Identification Sheet whilst it remains active. If this should become inactive it should be removed and filed in the Legal Section on the second spine. This must be recorded both in the paper and electronic record.

Identification Sheet (Front Sheet)

The identification sheet will contain the following information:

- NHS Number.
- Locally used Hospital Number.
- Surname and Forename.
- Home address, to include postcode.
- Telephone number, to include mobile where appropriate.
- Date of birth.
- Age.
- Gender.
- Civil Status.
- General Practitioner.
- Occupation.
- Birthplace.
- Religion.
- Ethnic Category.
- Next of kin details.

All of this information must be checked with the patient each time they attend the hospital and a new front sheet printed off and filed if any of the details change. The old front sheet must be removed and destroyed confidentially.

Labels

There must be adequate identification labels and specimen labels firmly secured in the front of the health record. If barcode labels have been printed these must also be firmly secured at the front of the health record. These labels must be legible and current, and checked that this information is still the most up to date, if this is not the case these labels must be replaced with the new details.

Divider Cards and Specialty Sheets

All clinical sheets are preceded with a specialty divider card and then secured onto the first spine. They are filed in chronological date order (as if you were reading a book); irrespective of which clinician the patient has seen within that specialty.

All correspondence is filed securely at the back of the clinical sheets, but still on the first spine but in reverse chronological date order. This means that the last letter will be opposite the last entry on the clinical sheet.

Surgical Specialties Only

At the end of the surgical specialties there should be an Operations and Anaesthetic specialty divider card, behind which sits the green operation notes and pink anaesthetic notes together and in reverse chronological date order – the most recent on the top

Information relating to a PALS enquiry/investigation or complaint **must not** be filed within the patient health record. PALS are a confidential service and information must not be disclosed unless the patient has given their expressed consent to do so.

Second Spine

Results are either filed on mounted sheets in date order from top to bottom, or A4 generated results are filed in front of the mount sheets. There remains a generic mount sheet for all other results not produced on A4.

All loose machine generated results such as CTG/ECG traces are to be placed in the wallet provided and filed in front of the results. Medical photographs will also be filed in this wallet. The front of the wallet must be completed to reflect the content and have a patient identification label affixed to it.

A Legal specialty divider card will be placed at the back of the results and all consent forms will be filed here in chronological date order – reading like a book. Also filed here will be living wills, advanced decisions, and consents for clinical trials. It will not contain anything pertaining to a PALS enquiry, complaint, litigation, Datix or adverse clinical incident.

Third Spine

Nursing documentation (sections 1-8) is filed on this spine, in chronological date order – reading like a book – and must be kept in episode order.

Information relating to a PALS enquiry/investigation or complaint **must not** be filed within the patient health record. PALS are a confidential service and information must not be disclosed unless the patient has given their expressed consent to do so.

Duplication and Version Control

There must only be one main health record registered and raised for each patient, duplication of records puts patients and the organisation at risk. Where it is unavoidable and temporary folders have to be raised the key identifiable information must be available so that merging of the records as soon as is possible can take place safely and the tracking system updated to reflect the amalgamation. Please refer to the RCHT Health Records Standard Operating Procedures.

There may be occasions when two or more records on the Patient Administration System appear to be for the same patient. In this instance the Data Quality Team **must** be contacted. The Data Quality Team will determine if the records are for the same patients and will merge the records into one, ensuring that any other records in existence, including electronic records, for the patients are merged at the same time.

If you need to change details on patients for the following reasons, you must contact Data Quality and they will manage these requests:

- Children under the age of 16.
- Multiple births.
- Adoption.
- Gender reassignment.
- Name change by deed poll.

There may be occasions where a patient is attending the following departments that hold departmental records for patients; these do not leave the departments:

- Renal Department.
- Sexual Health.
- Oncology.
- Therapies (whilst the patient is currently an outpatient).

Ring Binders for Inpatients

Generally, the main patient health record is kept in the Nurses/Doctors office on the ward and only a ring binder with the current episode of information is held in the secure notes trolley. Nursing records are also being held separately whilst patients are an inpatient; generally, these are outside of the bays in wall holders. This change in practice was in response to the main patient health record holding too much information and not always relevant to the current admission, it is expected to provide efficiencies in being able to access current information in a timely manner. The main patient record is always available for reference.

The Trust is committed to using the NHS number to uniquely identify patients.

Data Entry and Record Keeping

Health records serve many purposes; the most important is the contemporaneous record of events and assessments that assist diagnosis and treatment. It is important for these records to contain all relevant information about the patient so that any healthcare professional can continue the care of the patient. The following should form the basic standard of the health record. By adopting these standards RCHT is providing a framework to manage the risks associated with record keeping. The qualities of availability, accessibility, interpretation, and trustworthiness must be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

The record keeping standards are based upon the Academy of Medical Royal Colleges (AoMRC) shown below:

Standard Number	Description
1	The patient's complete medical record should be available at all times during their stay in hospital.
2	Every page in the medical record should include the patient's name, identification number (must include NHS number, may include local ID) and location in the hospital.
3	The contents of the medical record should have a standardised structure and layout.
4	Documentation within the medical record should reflect the continuum of patient care and should be viewable in chronological order.
5	Data recorded or communicated on admission, handover and discharge should be recorded using a standardised proforma.
6	Every entry in the medical record should be dated, timed (24-hour clock), legible and signed by the person making the entry. The name and designation of the person making the entry should be legibly printed against their signature. Deletions and alterations should be countersigned, dated, and timed.
7	Entries to the medical record should be made as soon as possible after the event to be documented (for example change in clinical state, ward round, investigation) and before the relevant staff member goes off duty. If there is a delay, the time of the event and the delay should be recorded.
8	Every entry in a medical record should identify the most senior healthcare professional present (who is responsible for decision making) at the time the entry is made.
9	On each occasion a transfer of care occurs, the consultant responsible for the patient's care will change the name of the responsible consultant and the date and time of the agreed transfer of care.
10	An entry should be made in the medical record whenever a patient is seen by a doctor. When there is no entry in the hospital record for more than four (4) days for acute medical care or seven (7) days for long-stay continuing care, the next entry should explain why.
11	The discharge record/discharge summary should be commenced at the time a patient is admitted to hospital.
12	Advanced Decisions to Refuse Treatment, Consent, and Cardiopulmonary Resuscitation decisions must be clearly recorded in the medical record. In circumstances where the patient is not the decision maker, that person should be identified e.g. Lasting Power of Attorney.

Generic Standards

Identification Data

There should be a single acute record in existence for each patient and it must be identified as such using the NHS number as the primary identifier and also the locally generated hospital number. On each side of every document there must be sufficient information so as to identify the patient, as a minimum the patient name, Date of Birth, NHS number and local Hospital CR number

Date and Time

Every entry should be dated and timed (using 24hour clock). This may be crucial when trying to reconstruct events and treatment given, maybe several years later.

Entries in the record are attributable

The entry must be attributable to an individual therefore printed name; along with designation as well as a signature must be part of every entry into the patient's records. The use of common identifiers for clinicians who write in the notes, such as the GMC number should be encouraged. Every entry should identify the most senior healthcare professional present who is responsible at the time the entry is made.

Assistant Practitioners (Band 4 within the nursing, midwifery and AHP professional groups) and Health Care Support Workers/Therapy Assistants (Band 3 and 2 within the nursing, midwifery and AHP professional groups) are able to document their individual care interventions and independently sign these entries directly into the health record (electronic or paper based).

There may be occasions when administrative staff need to document something in the patient record, examples such as recording where information has been challenged by a patient and the action taken.

Below are the staff that are authorised to enter and/or access information in a patient record.

Healthcare Professional	**Legitimate reason for access to personal identifiable information (irrespective of format)**
Clinical Staff: Consultants. Doctors. Nurses. Midwives. Allied Healthcare Professionals. Medical Students. Assistant Practitioners. Health Care Support Workers.	Treating/consulting with patients.

Healthcare Professional	Legitimate reason for access to personal identifiable information (irrespective of format)
Clinical Support Staff: Biomedical Scientists. Radiographers.	Diagnostic testing.
Administrative Staff: eHealth Records Manager (Operational). Medical Secretaries. Outpatient Booking staff. Reception staff. Ward Clerks. Clinic Preparation staff. eRecords Assistants. Disclosure Office staff. Access Co-ordinators. Clinical Coders.	Administratively supporting the patient pathway. Preparing records for Disclosure.
Management: Senior Management Team. Divisional Managers. Service Leads. Divisional Governance Leads. Information Asset Owners.	Respond to queries, complaints, and validation. Ensuring good quality of data and addressing if there are issues/concerns.
Support Services: Data Quality. Cornwall IT Services Help Desk. IT Security Manager. Chaplaincy Services.	Merging of duplicate records. Correcting administrative information on the Patient Administration System. Responding to information security incidents. Ensuring pastoral care is offered.
Legal Services Team	Responding to litigation queries. Protection of the Trust.
Records Services Management Team	Monitoring and auditing systems to ensure legitimate access to records. Responding to queries and complaints. Identifying information for release or viewing by patients. Recording actions in response to challenges made by patients regarding the content of their record.

Healthcare Professional	Legitimate reason for access to personal identifiable information (irrespective of format)
Audit and Research Teams	To provide assurance of implementation of policies and procedures and to monitor trials and research.
Complaints and Compliments Team	To support the complaints process. To facilitate Local Resolution Meetings.

Each time a patient is transferred to another consultant the name of the new consultant responsible and the date and time of the agreed transfer of care should be recorded.

Legibility

All entries must be legible and where at all possible written in black ink, this provides greater clarity when the records are being reproduced for disclosure and/or scanned. **Coloured pens must not be used.**

Complete

All episodes and interventions made in regard to a patient must be recorded as soon as possible after the event, this may be a hand-written entry or a typed entry. If there is a delay, the time of the event and the delay should be recorded.

An entry should be made whenever the patient is seen by a doctor. Where there is no entry in the record for more than four days for acute care or seven days for long-stay care, the next entry should explain why.

The record should reflect the continuum of patient care and should be viewable in a chronological order.

The content and context of the record must be able to be interpreted. The Trust must be able to form a reconstruction of activities or events that have taken place. There must be a full audit trail of all activity taking place.

The record reliably represents the information that was actually used in, or created by, the patient pathway, and its integrity and authenticity can be demonstrated.

Abbreviations

The use of abbreviations must be kept to a minimum. The only abbreviations used must be nationally approved by your different professional bodies. Healthcare professionals must be aware that an excepted abbreviation within their own clinical field may have a different interpretation in the wider field of clinical care. Where possible and appropriate the abbreviation should be written out in full the first time it is used.

Alterations

Entries in to the clinical/health record must never be erased, overwritten, or inked out. Errors should be crossed through with a single line; initialled, dated and timed thus ensuring unauthorised or inadvertent alteration or erasure does not take place. The reason must be clearly recorded why the entry has been crossed through. This also aids proper access and disclosure.

Entries recorded electronically must never be deleted or overwritten. Errors will be managed by following prescriptive procedures appropriate to the electronic system, but must include the following underlying principles:

- Wherever an electronic entry is made there must be provision to change it, it must not be deleted. It is desirable that changes should be visible by hovering over the data field and provision to record why the information is being changed.

- You must be able to see what was recorded prior to the change as well as the correct information.

Incorrect information recorded in the health record, which has been identified either by a member of staff or a patient must be logged on the Trust's Datix incident recording system. This can be in the form of a wrong document filed or a direct entry made within the clinical notes. Incorrect information identified in any of the electronic patient records must be brought to the attention of the Information Asset Owner to address, this is likely to be in conjunction with the Data Quality Team.

Any request by a patient to change/remove information must be directed to the Records Services Management Team to deal with.

Additions

Anything added to an entry at a later date must be separately dated, timed, and signed. The reason must be clearly recorded why the entry has been added at a later time and date.

Personal comments

Employees of the Trust must not use offensive observations about the patient's character, appearance, or habits. Patients/next of kin and representatives are allowed to access to records under the Data Protection Act 2018 and Access to Health Records Act 1990.

Dictated notes

These should be checked and signed by the professional who dictated them. It is not the responsibility of the person typing the notes.

Reports

Every report from a diagnostic examination should be seen and acknowledged by a clinician in either electronic or paper form. Results requiring an action should be recorded in the patient's clinical/health record along with the appropriate action taken.

Information given to patients

All patient information sheets must be clearly recorded in the patient's health record including title/reference number and date provided. You should not file the actual patient information, just reference it.

Relevant legal information

Mental capacity, healthcare professional must document the mental capacity of the patient to make decisions about treatment.

Advanced decisions to refuse treatment are written documents and should be completed and signed when a patient is legally competent to explain their wishes in advance, or to allow someone else to make decisions on their behalf.

Lasting power of attorney, this documents who is the person or deputy if there is a lasting power of attorney, this does cover health matters.

Enduring Power of Attorney predominantly covers financial and material things; it does not generally cover health unless it is regarding onward care to a home that involves financial information. For further guidance contact the Data Protection Officer or Records Services Manager.

Organ donation must record whether patient has given consent for organ donation.

Joint parental responsibility court orders or child arrangement orders must be directed through the Records Management Team to ensure that appropriate disclosure of records is identified as an alert on the child's record.

Access and Disclosure of Patient Records

All requests for access to or disclosure of personally identifiable information, including patient records must be directed to the Disclosure Office, See Appendix 7 for more detailed information.

Filing of Loose Documentation

It is **every employee's responsibility** when handling the health record to ensure all documentation is securely filed and fastened within before it is returned to the Health Records Department for filing or for onward transmission to another user/department.

Means of securing documentation may vary in the health record, but adhesive tape or staples **must not** be used. Any loose filing must be securely filed to ensure it is not lost during transportation between departments etc.

Complaints, litigation, and documentation relating to incidents **must not** be filed in the health record.

Where incorrect filing has been identified within a patient record it must be recorded using the Trust's Incident Reporting System, Datix, including as much information about the wrong information, who it belongs to and whose record it was found in. The information must not be removed. The Records Services Management Team or the Manager where the incident occurred will manage this through Datix. Where it is not clear what information belongs to which patient clinical assistance must be sought where the incident occurred to ensure that any changes are reflected appropriately and safely.

Where personal identifiable information has been found in inappropriate areas it must be handed into the nearest Reception Desk and reported using the Trust's Incident Reporting System, Datix. The Information Governance Team will manage this through Datix and will collect the identified information.

Clinical Document Management

The Forms Review Group agrees new and revised documents. This is a formal process that must be followed to ensure that the forms/documents/assessments contain the necessary information, follow a standard format where appropriate and to manage version control of documents being replaced. A checklist must be completed and sent to the Chair of the group along with a sample of the proposed document. The creator of the document will be invited to attend the group meeting to present their document. Further information is available on the Forms Website on the Trust's Intranet. The compliance of forms creation is vital as the Trust moves to a scanned record and can build eForms for direct data entry.

Monitoring compliance and effectiveness

Good record keeping ensures any decisions made can be justified or reconsidered at a later date, and it is clear what has been done, or not done, and why. This is of vital importance in providing quality patient care, and also in cases of clinical liability.

Objectives

- To provide evidence that this policy has been embedded throughout the organisation.
- To provide evidence of compliance with this policy.
- Improve the quality of the health record.
- To improve the standard of patient care through improved record keeping.
- Provides evidence of performance in specialty areas.
- To identify areas of improvement and document in an action plan.

Template

The Audit Template can be accessed on the Records Management Website (Inpatient Discharge Template) that can be found via the Trust's Intranet → A-Z Services → Records Management → Records Management Resources.

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	The Records Services Management Team will conduct monthly audits on ten health records following discharge to an inpatient stay. Over a twelve-month period, there should be evidence of multi-professional clinical audits against the policy standards of record-keeping for all professional groups in at least 50% of the services. The audit is based upon this policy and the standards at Appendix 1.
Lead	Records Services Manager
Tool	Ten health records will be identified from a report provided by Information Services on the previous month's discharged patients. The following sample of records is to be included: 1. A record of a deceased patient. 2. A record of a temporary resident. 3. A record of a patient discharged from West Cornwall Hospital. 4. A record of a patient discharged from St Michael's Hospital. 5. A selection of records from the following Surgical speciality: a. ENT. b. Oral Surgery. c. Ophthalmology. d. Breast (SMH). e. GI. f. Urology. g. Trauma/Orthopaedics (SMH). 6. A selection of records from the following Medical Specialty: a. Cardiology. b. Gastroenterology. c. Respiratory. d. Eldercare. e. Medical Admissions. f. Endocrine. g. Renal. h. Neurology. i. Emergency Department. 7. A selection of records from the following Speciality Medicine: a. Haematology.

Information Category	Detail of process and methodology for monitoring compliance
	b. Rheumatology. c. A selection of records from the following Women's and Children Specialty: d. Paediatric. e. Gynaecology. f. Obstetrics. There should be a 30/70 split of new style folders to old style folders. **Methodology** Information Services provide a report to the Health Records Library Supervisor on a monthly basis and health records are identified using the criteria above. The content of the audit is based upon the recommended audit tool of the Royal College of Physicians; this has been adapted to record a number of locally agreed criteria. The Records Management Team rigorously go through each health record and assess against each criterion as set out in the audit tool. The results of the audit are recorded manually in the first instance, documenting the details of the patient by use of a patient identification label. The results are then transferred electronically to an excel spreadsheet and anonymised for reporting purposes. From the audit five main areas are considered for improvement. From the audit three action points are recommended to improve the quality of clinical record keeping. The health records are returned for filing in the main health records library.
Frequency	Monthly
Reporting arrangements	**Information Governance Group** The audit forms part of the annual report that is presented to the Information Governance Group. **External Monitoring Bodies** The following bodies will expect to see the results of these audits as part of the external monitoring process: ▪ NHS Litigation Authority. ▪ Data Security and Protection Toolkit. ▪ Care Quality Commission.

Information Category	Detail of process and methodology for monitoring compliance
Acting on recommendations and Lead(s)	The Records Services, PAS and Data Quality Manager will undertake subsequent recommendations and action planning for any or all deficiencies and recommendations within reasonable timeframes. The subsequent action plan will identify the recommendation and a specified timeframe for implementation.
Change in practice and lessons to be shared	Any system or process changes or lessons learnt will be shared with the Information Governance Group. This will also be shared with Data Quality and Information Asset Owners as well as through the Daily Bulletin and For the Record publication. Following any change, the Records Services Manager will arrange to re-audit.

Appendix 6. Recordings and Photography Standards

Medical Recordings

Recordings, whether originating in the Medical Photography Department or using mobile devices purchased for departments use (and sometimes purchased from charitable funds), which illustrate a patient's condition or an aspect of the treatment, form a part of that patient's health record and are protected in the same way as any other health record.

In almost every situation staff should not use their personal devices to record images. The only exception to this would be where the image is time dependent, and no Trust approved device is available. Once the image has been transferred to the Trust storage area, the image must be deleted immediately. The person taking the images retains responsibility for that image whilst it is on their device.

Freelance professional photographers are sometimes employed to make this sort of recording. They may only be introduced to The Royal Cornwall Hospital NHS Trust by arrangement with the Press Officer or Director of Communications.

All equipment used for medical recordings must be purchased through the Cornwall IT Services Helpdesk. Your request will be logged, and the Records Services, PAS and Data Quality Manager will contact you to seek assurance of your compliance with this policy specifically around the use, storage, security, and access of images. Once this has been established approval will be given to purchase the equipment.

In the event of a digital photograph needing to be taken urgently out of normal office hours there is a digital camera available on the Neonatal Unit and the Emergency Department that may be used. They must be returned immediately once they have been finished with. It is the user's responsibility to ensure all images are removed from the device prior to them being returned.

Other Recordings

Any images taken by staff for personal reasons (not containing images of patients or service users) and those taken by patients and visitors must be done so with regard to the individuals' confidentiality, respect, and dignity.

An example where this maybe come an issue is if a patient is photographed in a clinic area and the image is posted to a social network site their confidentiality and Human Rights would have been compromised.

To take an image of a patient and post it to social media without consent or without legal justification could contravene Article 6 and Article 9 of the UK General Data Protection Regulation.

In this Act "sensitive personal data" means personal data consisting of information as to his/her physical or mental health condition.

Images taken could also contravene Article 8 of the Human Rights Act.

The Human Rights Act 1998 (HRA) enshrines the right to respect for private and family life set out in Article 8 of the European Convention on Human Rights (Convention) which states:

Everyone has the right to respect for his private and family life, his home, and his correspondence.

Nuisance - Criminal Justice and Immigration Act 2008 creates a new offence of causing nuisance or disturbance on NHS premises. A person may commit an offence if he or she causes, without reasonable excuse and whilst on NHS hospital premises, a nuisance or disturbance against an NHS staff member and refuses to leave when asked to do so by a police constable or NHS staff member.

Patients and visitors should only take images or recordings of consultations with staff after seeking explicit consent. Although this is not required by law, staff should have an expectation that whilst discharging their duties that their confidentiality is respected.

Patients should be informed that posting images on their social media could result in the staff member taking Civil action against them.

Patients, parents, carers, and other healthcare professionals may send in photographs or videos to the various healthcare professionals to show something that they are concerned about (rash, inflammation, swelling, gait etc). Sometimes the patient is clearly identifiable from the image. In these circumstances the person sending in the image must be made aware that this will form part of the health record and will be uploaded for future reference and must consent to this. Where it is possible the image/recording must be uploaded into the patient's electronic health record, however where this is not possible it must be stored on a secure drive and an entry into the patient record must be made to identify this to other healthcare professionals and to the Disclosure Office for Subject Access Requests.

Healthcare professionals are delivering care in a number of different ways since the covid pandemic and will become a normal way of delivering care. Attend Anywhere is the current provider of software allowing consultations to be carried out over video with the patient and in their own homes. Both parties need to be aware of their surroundings when in a consultation to protect their confidentiality. The recording will be managed the same way as any other recording, it will be uploaded into the patient's electronic health record, however where this is not possible it must be stored on a secure drive and an entry into the patient record must be made to identify this to other healthcare professionals and to the Disclosure Office for Subject Access Requests.

Confidentiality

Confidentiality is the patient's right and may usually only be waived by the patient or by someone legally entitled to do so on his/her behalf. You are reminded that breach of confidentiality may well amount to serious professional misconduct with inevitable disciplinary consequences and could result in substantial financial damages.

In order to ensure that the patient's right to confidentiality is preserved, The Royal Cornwall Hospital NHS Trust requires that:

- The patient's consent is obtained in writing for the original recording and for its use as a part of treatment or for teaching in Cornwall (with the exception of those listed in the section Recordings for which separate consent is not needed, which are exempt), or for further specified use, such as publication.

- Staff must not upload images or recordings to public domains of personal information relating to patients, colleagues, and visitors. An example of this would-be images of patients in hospital or comments made.

- It is the Trust's expectation that visitors and patients will not upload images or recordings of individuals in the hospital to public domains.

- The Medical Photography department will only produce copies of medical photographs upon receipt of the original consent form. Copies must only be made for official RCHT purposes, or as part of a disclosure under the DPA18 or Access to Health Records Act 1990; all disclosures must be managed through the Information Governance Office.

- Prior to publication in journals, books or elsewhere, the patient's permission for the specific use proposed is sought and written consent obtained.

- All projects/research involving recording patients must be registered with the Research Department as part of the overall research project.

Consent

Proper informed consent for recording and disclosure must be obtained if the recording is made as part of the assessment or treatment of patients. The most up to date consent forms for photography will be available on the forms to print page, accessible via the Trust's intranet. This must be recorded in the patient's health record for the general consent. A copy should be given to the patient and also the Medical Photography Department if appropriate.

The practice of obtaining the patient's written consent only in the case of full length or facial recordings, from which the patient can easily be identified, is not sufficient. It is sometimes possible for people to be identified from other categories of recording, e.g. showing a tattoo or other distinguishing mark. Nor is it sufficient to rely on the photographer or consultant's judgement that a particular patient is unlikely to be identified from a particular recording.

The Royal Cornwall Hospital NHS Trust has therefore adopted the policy that informed consent to recording is obtained from all patients and in all cases (except those that are exempt). Remember those recordings taken as part of treatment or assessment are part of the patient's health record and must be treated in the same way as written notes.

In the case of procedures, recording is implicit (e.g., endoscopy), consent to the procedure provides implicit consent to recording under normal conditions. Health professionals must ensure that they make clear in advance that photographic, or video recording will result from the procedure.

In all cases of recording, care must be taken to respect the dignity, ethnicity, and religious beliefs of the patient.

Patients have the right to withdraw consent for use of their recordings at any time. Patients should not be placed under pressure to give their consent for the recording to be made. If a patient decides to withdraw consent, the records must not be used and, if made in the context of teaching or publication, destroyed.

In the case of electronic publication, it should be made clear to the patient that once a recording is in the public domain; there is no opportunity for effective withdrawal of consent already given.

Children or young people

If children are competent to give consent for themselves, you should seek consent directly from them. The legal position regarding competence is different for children aged 16 and 17 and for those under 16. Children or young people over the age of 12 who are assessed as having the capacity and understanding to give consent for a recording may do so. However, they should be encouraged to involve their parents or those with parental responsibility in the decision making. Where a child or young person is not able to understand the nature, purpose, and possible consequences of the recording you must obtain consent from a person with parental responsibility.

Recordings of children or young people should only be taken if there are specific features that need recording for clinical reasons (e.g., assessing the progression of a skin lesion) or teaching (e.g., an important clinical sign that might only be seen rarely). Recordings should only include the specific areas of interest; whole body images should only be taken if completely necessary. Recordings of genital areas must only be taken if deemed absolutely necessary and appropriate. Recordings of the chest in peri or post pubescent girls must only be taken if deemed absolutely necessary. It is strongly recommended that a clear indication be recorded in the patient's health record justifying the recording in both of these events.

In cases where a video or audio recording are to be made and the child is deemed to be of an age and understanding to give consent then their consent should be recorded on the video/audio at the beginning of the recording.

Unconscious Patients

Photographs of unconscious patients may only be taken with consent from the next of kin/personal representative. Once the patient has regained consciousness, they must be informed that a photograph has been taken and if they object to the use of the photograph, it must be destroyed. This must all be documented in the patient's health record.

Psychiatric Patients

The recording – especially on video – of psychiatric patients requires particular care; guidelines for these procedures have been published by the Institute of Medical Illustrators (Code of Responsible Practice, published 1996 and updated 1998, available from The Hon. Secretary, Institute of Medical Illustrators, Medical and Dental Illustration Unit, Leeds Dental Institute, Clarendon Way, Leeds, LS2 9LU).

Patients who lack capacity

If you judge that an adult patient lacks capacity to consent to an investigation or procedure which involves a recording, you must obtain consent from someone who has legal authority to make the decision on the patient's behalf before making the recording. If there is no legal authority to make the decision on a patient's behalf, or where treatment must be provided immediately, recordings may still be made where they form an integral part of an investigation or treatment that you are providing in accordance with the relevant legislation or common law. Note: Powers of Attorney does not necessarily extend to authority over health matters; if you need further guidance on this please contact the Data Protection Officer or Records Services Manager.

In the case of recordings for secondary purposes, you must not assume that because a patient lacks capacity to make some decisions that they lack capacity to make any decisions at all or will not be able to make the decision in the future. Before deciding if patients have capacity to make a decision, you must take all practical and appropriate steps to enable them to make the decision for themselves and considering the use of simple language or visual aids or by involving a carer, family member or personal representative.

For further advice about involving adults who lack capacity, in research where recordings may form part of the research, see GMC Guidance on Consent to Research.

Deceased Patients

If a patient dies before a retrospective consent can be obtained, material by which the patient is identifiable can only be released with the consent of the deceased's personal legal representatives. You should follow a patient's known wishes after their death. You are reminded that the duty of confidentiality survives the death of the patient and you and the Trust can be prosecuted under the Access to Health Records Act 1990.

If a consenting patient subsequently dies, permission should be sought for any new use outside the terms of the existing consent. In this instance the consent of the personal representative is required.

If the recording will be in the public domain or the patient is identifiable you will need to consider whether the patient's family should be consulted. For further guidance you should seek legal advice through the Data Protection Officer or Records Services Manager or from your medical defence organisation.

Post-Mortem Examinations

Post-mortem examinations are governed by legislation in the UK. Recordings may form an integral part of a post-mortem examination and separate consent is not needed for making recordings of body organs, body parts or pathology slides to assist in the cause of death. However, relatives should expect that information is given to them to explain why a recording may be made. If you wish to make recordings for secondary purposes such as training, teaching, or research you should seek consent at the same time you seek consent to undertake the examination. If you have not foreseen this possibility, you may make recordings for secondary purposes without consent provided that they do not include images that might identify the person. In the case of a Coroner's post-mortem consent must be sought from the Coroner to use the information. Recordings can only be taken on specific Trust equipment and by nominated individuals. A record is kept of all recordings taken.

Non-Clinical Recording

In cases where the patient is incidental to a recording, e.g., where the picture is to illustrate a particular equipment set-up, consent to appear in the recording is still required from any patient, member of the public or staff. Members of staff who normally operate the equipment in a recording are deemed to have given their consent to the recording and its further use by appearing in the recording. If the member of staff does not normally work in that area, then consent should be obtained and filed.

This should be specific and detailed as described in the ‘Confidentiality’ section above.

Accidental recording of patients, members of the public and staff do not require consent to use their images, for example people walking along a corridor or a general picture of a ward/department area.

There may be occasions where meetings are recorded, for example in the case of Local Resolution Meetings in response to a formal complaint or a general meeting within the hospital where this is used to type the minutes of the meeting. In these cases, consent within the group attending the meeting should be sought. Once the notes/minutes have been typed and ratified the recording should be disposed of in line with Trust Policy if recorded by the Trust. Patients attending Local Resolution meetings may well bring their own recording equipment, providing all attending consent to this taking place then this should be allowed.

Recordings may be made to aid consultation and the patient may be given a copy of the recording. These requests must be managed through the Disclosure Office.

Recordings for which separate consent is not needed

You do not need to seek permission to make the recordings listed below, nor do you need consent to use them for any purpose, provided that, before use, the recordings are effectively anonymised by the removal of any identifying marks:

- Images taken from pathology slides.
- Clinical images (x-rays).
- Laparoscopic and endoscopic images.
- Images of internal organs.
- Recordings of organ functions.
- Ultrasound images.
- CT.
- MRI.
- Nuclear Medicine Images.
- Radionuclide Imaging.

Such recordings will not identify the patient. It may nonetheless be appropriate to explain to the patient, as part of the process of obtaining consent to the treatment or assessment procedure that a recording will be made. You may disclose or use any of the above recordings for secondary purposes without seeking consent provided that, before use, the recordings are anonymised.

In exceptional circumstances, recording may be necessary without consent, for example in the case of a child with injuries where abuse is suspected. A person with parental responsibility should be informed of the reasons for clinical photography and should be given the opportunity to consent. The parents’ responses should be recorded. The agreement of

the child, if of sufficient understanding should also be sought. In the absence of parental consent, photography should be authorised only by a senior doctor with child protection responsibility for the case. Recordings taken in these cases may be required as evidence in criminal or public proceedings and no absolute guarantees of confidentiality in this respect can be given.

Recordings made for research, teaching, training, and other healthcare-related purposes

To address the issue of existing collections that are used for teaching and training, you may continue to use anonymised recordings as well as those that identify the patient as long as you have a record that consent was obtained for the recording to be made or used. You must not use recordings for which there is no record of whether consent was obtained where it is clear from the context that consent had not been given to the recording or the patient is, or may be, identifiable.

For current recordings you must obtain consent for teaching, training, the assessment of healthcare professionals and students, research, or other related healthcare-related purposes. It is always good practice to get written consent, but verbal consent is considered sufficient if written consent is not practicable. Either consent should be stored with the recording.

Recordings for use in widely accessible public media (television, radio, internet, print)

You must obtain the patient's consent, which should usually be in writing to make a recording that will be used in widely accessible media, whether or not you think the patient will be identifiable from the recording. If the recording was anonymised, it is still considered to be good practice to seek consent before publishing it. Before any arrangement is made to undertake such recordings, you must obtain agreement from your employer, you must contact the Press Officer to see if such a contract exists. Patients must understand that once they have agreed to the recording being made for broadcast, they may not be able to stop it subsequent use. If the patient wishes to restrict the use of the recording, they should be advised to get agreement in writing from the programme maker and the owners of the recording, before recording begins.

You must not participate in making or disclosing recordings of children or young people who lack capacity, where you believe that they may be harmed or distressed by making the recording, even if the person with parental responsibility has given consent. Contact the senior doctor with child protection responsibility for the case for advice.

Recordings of adults who lack capacity that have been made in accordance with legal requirements may be disclosed for use in the public media, where this can be justified in the public interest. Where a person has legal authority to act on behalf of the patient, they will need to assess and decide whether disclosure is justified in the public interest.

Making recordings covertly

Covert recordings should be undertaken only when there is no other way of obtaining information which is necessary to investigate or prosecute a serious crime, or to protect someone from serious harm, as in the case of suspected child abuse. Before any covert recording can be made, authorisation must be sought from Trust senior management guided by the Trust's named professionals for safeguarding. In most cases covert recordings will be carried out by the Police and falls in the scope of the Regulation of Investigatory Powers Act 2000.

Recording telephone calls

Telephone calls from patients to healthcare organisations may be recorded for legitimate reasons such as medico legal, training and audit as long as you have taken all reasonable steps to inform the caller that their call may be recorded. You must not make secret recordings of patients.

Processing

It is recognised that while digitally originated recordings are intrinsically no different to traditional recordings; they are easier to copy in electronic form and are therefore more at risk of both image manipulation and inappropriate distribution. Particular care must be taken to protect the image and maintain its integrity.

A patient's image may not be altered in any way to achieve anonymity and so avoid the need for consent. Blacking out of the eyes in a facial photograph is not acceptable means of anonymising the image.

Where digital photography is to be used to record images of patients, due care must be given before the start to ensure that the quality of the image (in terms of both resolution and colour depth) is adequate for purpose.

In order to maintain the integrity of the image, manipulation may only be carried out to the whole image, and must be limited to simple sharpening, adjustment of contrast and brightness and correction of colour balance.

Images of patients may only be transferred to approved Trust computers for use in connection with Ethical Committee approved and Data registered research projects or for the preparation of teaching materials for use in accordance with the 'Confidentiality' section above. All images must be anonymised prior to transfer to non-approved personal computers in the case of teaching.

It is recognised that images issued by the Clinical Imaging Department may not be in the best format for reproduction, it is the requirement of many journals that there is radiological input with the Radiologists preparing the images for publication prior to the capture in photographic or digital form. In all cases of reproduction, the Royal Cornwall Hospital NHS Trust retains both the right to approve the quality, relevance and accuracy of the images and their copyright.

Requests for recordings from the Medical Photography Department must be made on the approved request form at Appendix 6.

Requests for recordings of private patients must first be processed through the Outpatient Services Manager before being sent to the Medical Photography Department.

Storage and disposal

All recordings of patients must be stored on Trust premises. Negatives, master transparencies, original digital camera files and videotapes must be logged and stored on Trust supplied secure servers (never on your local machine). In the case of digital cameras, the files must not be manipulated in any way (including compression) before storage.

Recordings that may be considered ‘highly sensitive’ (child abuse for example, or neonatal deaths) must be given due consideration as to how and where these are stored. Access to these recordings must be restricted to those staff that have specific authority to access them. Please refer to the Records Services Manager for advice.

Since any health record has to be available for disclosure if required, it is essential that every recording is properly logged in the patient health record, along with the file location. Each recording must be labelled so as to uniquely identify the patient.

In the case of hard copy photographic negatives and transparencies, these must be securely stored and logically catalogued within the department that the recording was taken.

Historically images were stored on CD/DVDs, if you cannot locate an image within the patient health record this may be accessed through the Disclosure Office.

Since recordings are considered to be part of the patient health record all appropriate criteria pertaining to health records must be taken into consideration before any form of disposal takes place. The Retention Schedule contains guidance on the retention and disposal of all health records, which can be found on the Document Library on the Trust’s Intranet.

Disclosure of Recordings

Recordings made as part of the patient’s care form part of the Health Record and should be treated in the same way as written material in terms of security and decisions to disclose information. All requests to disclose recording must be channelled through the Information Governance Office.

Personal recordings made by staff.

Staff must not make a recording or take images which are not required as part of their legitimate role which includes patients, carers, visitors, or colleagues. No images of patients, carers, visitors, or staff should be made available via electronic means to others, including the use of messaging software of social media platforms.

Copyright

Copyright of all recordings taken by Trust staff in the course of their duties is vested in the Royal Cornwall Hospital NHS Trust.

Recording for media purposes or in instances where the Trust allows its buildings to be used as filming locations the copyright is retained by the production company.

Contracts with outside photographers must ensure that that they waive ownership of copyright and moral rights in the recordings they prepare, although they may still be allowed to reproduce the recording or medical image providing permission has been given from the Royal Cornwall Hospital NHS Trust on each individual occasion. It is important that in any contract for publication the copyright in the recording remains with the Trust and does not pass automatically to the publishers on first publication, otherwise the Trust might well find itself unable to protect the patient’s interests by exercising control over further publication of the recording.

Those signing contracts with book or other publishers have a responsibility to delete from the contract any suggestion that the copyright will pass to the publishers.

Junior doctors and others acquiring copies of recordings in the course of their duties may retain these for teaching purposes but must undertake only to use them within the terms of the original consent (see the section on 'Confidentiality' above). Copyright and reproduction rights at all times remain with The Royal Cornwall Hospital NHS Trust.

Copies of recordings must not be excessive and may be made only after discussion with the Medical Photography Department; decisions will be made case by case and on its own merit.

Before leaving the employment of the Trust, staff must seek specific permission to retain images for teaching purposes from the Data Protection Officer. The Royal Cornwall Hospital NHS Trust may grant such permission subject to the retention of copyright and all reproduction rights.

Dissemination and Implementation

This policy will be disseminated to all Trust staff members via the Document Library and via routine communications, such as team briefings and 'all-users' emails, with Senior Management, Line Managers, Records Management Leads, Information Asset Owners, and staff members. The previous version of this policy will be archived within the Document Library.

The Trust will ensure that this policy has been implemented through spot checks carried out by the Trust's Records Services Department and audit.

Monitoring compliance and effectiveness

The requirements of this policy will be subject to audit and spot checks. 'Reporting by Exception' will be employed in routine reports on the effectiveness of the arrangements contained within this policy provided to the Information Governance Group.

Information Category	**Detail of process and methodology for monitoring compliance**
Element to be monitored	Has the recording been stored on a Trust server and appropriate access controls been applied? It is unacceptable to store images on mobile phones. Has the recording taken been documented in the patient paper health record along with the location? Has consent been obtained and filed in the patient paper health record.
Lead	Records Services Manager

Information Category	Detail of process and methodology for monitoring compliance
Tool	**Methodology** Maintain a record of which departments have notified the Records Services Manager of recordings being made and their locations. Cross reference with patient paper health record to see if this image was recorded in the record and the location of the stored image for future disclosures. Complete an audit form detailing location, access, and reference to patient record.
Frequency	Quarterly. Over a twelve-month period, a sample of recordings will be audited for all Divisions.
Reporting arrangements	Information Governance Group. The Report is presented to the Information Governance Group for information by the Records Services Manager.
Acting on recommendations and Lead(s)	The Records Services Manager will undertake subsequent recommendations and action planning for any or all deficiencies and recommendations within reasonable timeframes. The subsequent action plan will identify the recommendation and a specified timeframe for implementation.
Change in practice and lessons to be shared	Any system or process changes or lessons learnt will be shared with the Information Governance Group. This will also be shared with the Data Quality and Information Asset Owners as well as through the Daily Bulletin and For the Record publication. Following any change, the Records Services Manager will arrange to re-audit.

Appendix 7. Access to and Disclosure of Personal Identifiable Data (PID)

Formal Application to Personal Information

All RCHT employees and staff who manage RCHT patient records, are expected to recognise a request for information from an individual and understand to whom a request should be directed. All formal requests must be made in writing and directed to the Information Governance Office in the Knowledge Spa. Rch-tr.disclosure@nhs.net

Applications to personal identifiable information are made under the following acts:

- DPA18 for living persons.
- UK General Data Protection Regulation for living persons.
- Access to Health Records Act 1990 for deceased individuals.

The Information Governance Office will record all formal requests for access to/disclosure of all personal identifiable information, but Finance will prepare and send out their information independently of the Information Governance Office.

A member of staff, patient, or their representatives with the individual's consent, has the right to apply for access to their personal identifiable information; this is known as a Subject Access Request. All requests should be made in writing and include the staff member/patient's signature. If a request is received from a staff member/patient's representative the individual must authorise the release of their information. The staff member/patient's representative may be a relative, friend, legal representative, or any other person that they consent to have access to their information.

If an individual is unable to authorise the release of their information due to a lack of mental capacity then a person who has been legally appointed to act on their behalf has the right to apply for access to the information of that individual. Such a person should be asked to produce evidence that they hold a lasting power of attorney or other legal basis which allows the person to make decisions regarding finances, property, and welfare.

The applicant has a right to an explanation of any terms in the information that they do not understand, for example, technical language or medical terminology.

Staff must not access their own health record or staff record or records of their family, friends, colleagues, or those known to them (even if they have consented) that they do not have a legitimate work reason to access the information, this could lead to disciplinary proceedings.

Power of Attorney

Where a request is made by an individual who has Power of Attorney this should be returned to the requestor as this predominantly gives authority where an individual lacks capacity with regard to financial and material management of their affairs. Consideration may be given where concerns of care could influence a change of location for the patient particularly if the new location is in non-state funded care. In this case you may consider asking the clinician concerned whether they could provide a written report. A copy of the document must be asked for, ensuring that it has been registered with the Office of the

Public Guardian and that a ‘welfare’ power is included. Records may not be released unless the welfare power is documented.

Deputyship

The requestor would need to be appointed by the Court and has been given authority over the patient’s healthcare and welfare as well as financial affairs. Reference ‘A Guide for Deputies appointed by the Court of Protection’ can be accessed via the Internet Site of The Office of the Public Guardian.

Litigation Friends

Where a patient is known to lack capacity either through being a minor or an adult who permanently lacks capacity to make decisions and litigation is contemplated, the request for records maybe through a Litigation Friend. A Litigation Friend’ appointment will be confirmed by the Court should litigation proceed however prior to a formal claim commencing records may be requested. It is in order to permit access to records by solicitors in this case.

Independent Mental Capacity Advocate

An Independent Mental Capacity Advocate (IMCA) is a statutory form of advocacy that provides safeguards for people who lack capacity to make decisions about:

- Serious medical treatment or,
- Moving into, or between, care settings (including hospital).

An IMCA is entitled under the Mental Capacity Act (2005) to ask for access to the person’s medical and health records, and to take copies from these.

The application must clearly identify the patient in question, and the records required,

including the following details:

- Full name – including previous names.
- Address – including previous address(es).
- NHS number (if available).
- Dates of records required.

Independent Mental Health Advocates (IMHA) are appointed for patients with mental health problems in a similar way to IMCAs and are statutorily permitted access to a mental health patient’s records on the patient’s behalf. Where an individual seeks access to their own information, the Trust should ensure that sufficient identity checks are carried out to ensure that they are satisfied that the patient is entitled to the information they are seeking. See section ‘Confirming Identity for Further Details’.

Access to children's personal identifiable information

Legally, young people aged 16 and 17 are regarded as adults for the purposes of consent to treatment and the right to confidentiality. As such, if a patient of this age wishes a health professional to keep any aspect of treatment confidential, this wish should be respected.

Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be disclosed. Case law has established that such a child identified in Fraser Guidelines (previously known as 'Gillick Competent'), i.e., where a child is under 16 but has sufficient understanding in relation to the proposed treatment to give, or without consent, consent or refusal should be respected. However good practice dictates that the child should be encouraged to involve parents or those with parental responsibility in their treatment. Parents can make subject access requests on behalf of their children who are too young to make their own request. A young person aged 12 or above is generally considered mature enough to understand what a subject access request is. They can make their own request and would need to provide their consent to allow their parents to make the request for them.

Parents making direct subject access requests to their children's records must first seek consent if the child has capacity and is over 12 years of age.

Referenced in the Children Acts (1989) and (2004), a child is anyone who has not yet reached their 18th birthday. 'Children' therefore means 'children and young people' throughout. The fact that a child has become sixteen years of age is living independently or is in Further Education, or is a member of the armed forces, or is in hospital, or in prison or a young offender's institution does not change their status or their entitlement to services or protection under the Children Act (1989).

If a parent or a person authorised with parental responsibility is applying for access to their child's personal identifiable information, the health professional should consider if the child is legally competent to make decisions regarding their healthcare, and if they have sufficient understanding and intelligence to enable him or her to understand fully what is proposed.

Parental responsibility for a child is defined in the Children Act (1989) as 'all the rights, duties and powers, responsibilities and authority which by law a parent of a child has in relation to the child and his property'. Parental responsibility can also be acquired by the local authorities if the child is under a care order.

Parental responsibility would include:

- Safeguarding and promoting a child's health, development, and welfare.
- Financially supporting the child.
- Maintaining direct and regular contact with the child.

Parental access must not be given where it conflicts with the child's best interests and any information that a child revealed in the expectation that it would not be disclosed should not be released unless it is in the child's best interests to do so.

Establishing parental responsibility, (where parents are separated and one of them applies for access to the records) can be complex and staff should always consider whether evidence of parental responsibility is required before information is shared. Where there are any concerns about establishing whether someone has parental responsibility, the Data Protection Officer should be contacted for advice.

If you are in any doubt at all as to whether information may be disclosed or accessed, you must seek further advice and guidance from the Trust's Data Protection Officer, Caldicott Guardian or Records Services Manager.

Format of the copied records

Any paper records will be produced in an electronic format unless otherwise stated. This may incur an administrative charge for a paper format. The Trust's preferred method of transfer will be by using Kiteworks or in some circumstances an optical disk. Clinical Images will be saved to a DVD and not reproduced in a hard copy format.

Informal Application to Personal Identifiable Information

The Trust encourages health professionals to give informal access to patients, where possible. Informal access should be restricted to current records written by the health professional approached for access.

An individual may **verbally** ask the health professional treating them, for access to their information in their presence and to discuss it with them. These requests are not formal applications under the Data Protection Act and may be done at any time during the patient's care. This would also apply to staff wanting incidental information held in their staff record.

No third-party information must be accessed/disclosed.

Please note that if the individual would then like a copy of the information you must follow the formal application procedure. Template request forms are available at the 'Request for Access to Personal Data' Form.

Other types of access/disclosure requests

Coroner's Office

Information may be disclosed to the Coroner if this information is being disclosed as original records from the Mortuary or Bereavement Office a form must be signed to transfer responsibility for confidentiality whilst in their possession. This form will also act as a receipt for the Trust that the original records are with the Coroner, they must still be tracked using the normal processes.

NHS Hospitals

Requests for personal identifiable information from other NHS organisations must made be in writing on letter headed paper, so identifying the requesting organisation. Once satisfied that this is a bona fide request information may be copied and sent.

Exception: Derriford Hospital – the main RCHT patient record may be sent to this hospital when the patient is attending, but the member of staff sending the records must inform the Health Records Library to enable them to monitor the return of the records. The member of staff sending the records must ensure that they are appropriately tracked on the Patient Administration System.

Independent Treatment Centres and the Peninsula treatment Centre

Information may be disclosed to these centres but only copies, not the original.

Other NHS Hospitals

Information may be disclosed to NHS hospitals but only copies, not the original (with the exception of University Hospitals Plymouth).

Records needed for translation

The Trust recognises the need on occasions to disclose personal identifiable information to outside companies who provide translation services. Any requests for this must first be directed to Divisional Managers and the current procedure followed which can be accessed on the Trust's Intranet.

Information Required for Private Consultations

Whilst the Disclosure Office will make every effort to meet the needs of individuals needing copies of their information for private consultations they are politely reminded to allow sufficient time to be processed under the Data Protection Act 2018, which is 30 days.

Civil Litigation Pre-Action Protocol

A pre action protocol is where records are requested by the patient or representative solicitor in contemplation of a claim and should provide sufficient information to alert the Trust where an adverse outcome has been serious or had serious consequences and should be as specific as possible regarding the records to be disclosed. These types of disclosures are jointly managed by the Legal Services department and the Information Governance Office.

By other Agencies

There will be occasions where the Trust receives requests for access to patient's records from other Agencies. These may include, the Police, the General Medical Council, Social Services and other NHS organisations or statutory bodies such as the National Health Service Litigation Authority (NHSLA) and Care Quality Commission. All of these requests must be managed through the Information Governance Office.

Police

The Police do not have automatic right of access to personal identifiable information; all requests from Police must be directed to the Information Governance Office or the Data Protection Officer.

Routine requests for police reports accompanied by consent from the data subject are handled by the Information Governance Office.

Requests for reports without data subject consent must be requested by the police using Section 29 of the Data Protection Act 2018 made to the Data Protection Officer.

Exchange of information without consent in connection with Serious Crime (murder, grievous bodily harm, rape, and other defined crimes) may be released to the police through the Data Protection Officer.

If the request from police occurs outside of normal working office hours and the disclosure is in connection with a serious crime then the senior manager on call must be contacted.

All efforts must be made to not allow the original record to be taken, and where possible to delay any disclosure until the staff in the Disclosure Office are on duty and can copy the records.

The Trust will consider carefully when information can be shared with other agencies and whether consent from a patient can and should be taken beforehand. Information Sharing protocols with the police and other agencies exist and any other information requests from the police or other public bodies will be considered under these protocols by the Data Protection Officer

Disclosures made to the Police will generally be done through Streamlined Forensic Reporting (SFR) software by the Information Governance Team. There will be occasions where this process is not followed, but that will be determined on a case-by-case basis by the Information Governance management team.

Death in Custody and Rule 43 Investigations

Any healthcare issues relating to Death in Custody Investigations and Rule 43 reports are the responsibility of NHS England Commissioners to progress working closely with the Prison Probation Ombudsmen's clinical reviewer. These reviewers are especially commissioned to undertake this work and operate within statutory codes of conduct with respect of confidentiality. Release of such records should be released when requested within the time scales stipulated.

Third Party disclosure

Where requests for patients' records are received from a third party, the Trust will consider the request carefully and on a case-by-case basis.

Where records contain information that relates to an identifiable third party, that information may not be released unless:

- The third party is a health professional who has compiled or contributed to the personal identifiable information, or who has been involved in the care of the patient.
- The third party, who is not a health professional, gives their consent to the disclosure of that information.
- It is reasonable to dispense with the third party's consent (taking into account the duty of confidentiality owed to the other individual, any steps taken to seek his/her consent, whether he/she is capable of giving consent and whether consent has been expressly refused).

Patients Living Abroad

Under the Data Protection Act 2018, former patients now living outside of the United Kingdom have the same rights to apply for access to their UK personal identifiable information. A request for access to personal identifiable information will be treated in the same way as a request made from within the UK.

Legitimate access controls to patient records

The accessing and sharing of information is strictly on a need-to-know basis. Individuals must be able to demonstrate that they have a legitimate association with the patient in the delivery of their job. It is recognised that it is not only healthcare professionals that need to have this access. The table below details those staff who will have a legitimate reason to access personal identifiable information.

Healthcare Professional	Legitimate reason for access to personal identifiable data (irrespective of format)
Clinical Staff: Consultants. Doctors. Nurses. Therapists. Medical Students.	Treating/consulting with patients.
Clinical Support Staff: Biomedical Scientists. Radiographers.	Diagnostic testing.
Administrative Staff Medical Secretaries. Outpatient Booking staff. Reception staff. Ward Clerks. Clinic Preparation staff. Health Records Library Operatives. Disclosure Office staff. Access Co-ordinators. Clinical Coders.	Administratively supporting the patient Pathway.
Management: Senior Management Team. Divisional Managers. Service Leads.	Respond to queries, complaints, and Validation
Support Services: Data Quality. Cornwall IT Services Help Desk. IT Security Manager.	Merging of duplicate records. Correcting administrative information on the Patient Administration System. Responding to information security incidents.

Healthcare Professional	Legitimate reason for access to personal identifiable data (irrespective of format)
Legal Services Team	Responding to litigation queries. Protection of the Trust.
Records Management Team	Monitoring and auditing systems to ensure legitimate access to records.
Audit and Research Teams	To provide assurance of implementation of policies and procedures and to monitor trials and research.
Line Managers	Maintenance of staff records.
Complaints and Compliments Team	To support the complaints process. To facilitate Local Resolution Meetings.

Exemptions

An individual has a general right to access information about themselves under the DPA18, held by the Trust. There are limited circumstances in which the Trust may determine that information cannot be provided to an individual who has made a request.

These circumstances include:

- In the opinion of the relevant health professional, the information to be disclosed would be likely to cause serious harm to the physical or mental health of the applicant or any other person.
- Where the record relates to, or has been provided by, an identifiable third party, unless the third party has consented to disclosure.
- The granting of access to a patient representative would disclose information provided by the patient, in the expectation that it would not be disclosed to the person making the request.
- The granting of access would disclose information obtained as a result of any examination or investigation to which the patient consented, in the expectation that the information would not be so disclosed to another individual.
- The patient has expressly indicated that such information should not be disclosed to another individual.
- Where disclosure may hamper the prevention or detection of serious crime.

- To avoid prejudicing the carrying out of professional/clinical work by causing serious harm to the physical or mental health or condition of the data subject or another person.
- Where other enactments themselves prevent disclosure e.g. adoption records and reports.
- Where an access request has previously been met the Act permits that a subsequent identical or similar request does not have to be fulfilled unless a reasonable time interval has elapsed between.
- Genito-urinary department records relating to sexual health. These are managed from within the department.
- Any information which is restricted by law from disclosure under other Acts of Parliament, which includes:
    - Human Fertilisation and Embryology Act 1990.
    - Human Fertilisation and Embryology (Disclosure of Information Act) 1992.
    - NHS (Venereal Diseases) Regulations 1974.
    - NHS Trust (Venereal Diseases) Regulations 1991.
    - The Abortion Regulations 1991.

There may also be occasions where a representative (such as a family member) who does not have an automatic right of access to the record, seeks disclosure. Whilst there is no right for next of kin to review the records of an incapacitated patient, there may be circumstances where it is appropriate. Where requests of this nature are made, they must always be considered on a case-by-case basis and should be referred to the Legal Services Department and/or Data Protection Officer.

Fees

Fees may be applied where requests are considered to be manifestly unfounded.

Viewing of records can be arranged through the Disclosure Office and usually takes place in the Health Records department.

Under the Access to Health Records Act 1990

There is no fee for accessing the health records of the deceased.

Timescales

The Data Protection Act 2018 requires requests to be complied with within 30 days and in exceptional circumstances if it is not possible to comply within this period then the applicant should be informed. If the person has been receiving treatment during the preceding 30 days, no more than 21 calendar days must elapse between receiving the written request for access (which must include the consent to release were applicable) and the records being released. If treatment was last given over 30 days ago then no more than 30 calendar days must elapse after the application has been made before access is given.

Where a request is considered complex a further period of 60 days can be applied. A complex request is where the disclosure would require access to multiple physical records and multiple IT Systems in order to collate the requested information. Requestors must be informed that there could be a delay in responding to the request when acknowledging receipt of the request.

The Access to Health Records Act 1990 requires that requests be complied with within 21 days where the record has been amended within the previous 30 days. If treatment was last given over 30 days ago then no more than 30 calendar days must elapse after the application has been made before access is given. Where a request involves excessive records or systems an extension of up to 60 days may be applied and the requestor must be informed within 30 days.

The 21 and 30 calendar days periods do not start until the written request and payment has been received in full and the identity or authority of the person making the request can be validated. In exceptional circumstances these timescales can be extended by mutual agreement of both parties.

Consents from third parties should be sought to fit within this 30-calendar day's period.

Access can be refused where the Trust has previously complied with an identical or similar request from the same individual unless a reasonable interval has elapsed between compliance with the initial request and the receipt of a further request.

Recording the Access Request

Any formal request for access to or disclosure of personal identifiable information must be sent to the Disclosure Office who will enter the information onto the Trust's Risk Management database. Through the integrated nature of this database, when a request is entered against an individual's name, date of birth or unique identifier, the database will flag up if there are any other open records in the Claims, Inquests, Incidents and Complaints modules which match the individual's information. Open records in any of the modules serve as a prompt for the staff to verify if the request needs to be made to other departments before completing the request.

Confirming Identity

Once a request has been made (or consent has been obtained where appropriate) due consideration must be given to the information submitted to confirm the identity of the individual, e.g. full and previous name, date of birth, current and previous address, unique identifying number, etc.

To ensure the Trust is satisfied as to the identity of the individual or applicant, a request for evidence of identity may be made. This could include a copy of a passport, driving licence, birth certificate, paid utility bill or any document that might reasonably be only in their possession. If the requester is applying for records on behalf of an individual, they will need to provide proof of identity (as above) and must also include the individual's written authorisation for access to their records.

If the requester is applying for the records of a deceased individual, they must include proof of their own identity together with proof of a court appointment as legal representative.

The Trust should check with the applicant to confirm what material is required before processing the request. The applicant does not have to give a reason for requesting access unless the claim is against the Estate and is being brought by someone other than the legal representative.

Correcting a Record – The Right to Rectification

If, after accessing the record, the patient/representative feels that information recorded on their health record is incorrect then they should be advised to discuss the situation with the health professional in an attempt to have the record amended. If the matter is not resolved they should contact the Records Services Manager who will be able to advise of the different options available. If this is still not resolved the patient/representative is to be advised of the current complaints policy and procedure as outlined in the Trust's Complaints Policy.

The Trust suggests in line with good practice that the individual is allowed to include a statement in their record that they disagree with specific parts of their record. The individual could seek further advice from the Information Commissioner, who may rule that any erroneous information is rectified, blocked, erased, or destroyed, or that legal independent advice should be sought, to pursue their complaint.

The ICO's office address is:

Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

ICO helpline (open between the hours of 9.00am and 5.00pm, Monday to Friday):

08456 30 60 60.

01625 54 57 45.

Fax: 01625 524510.

What Information is considered for disclosure?

Staff in the Disclosure Office will use the following table to ensure that if individuals have attended any of the following specialties as patients, then the Information Asset Owners/System Managers will be contacted to retrieve and make available any information stored therein. Information Asser Owners/System Managers will ensure that information sent relates to the individual in question.

System Name	Specialty
Oceano	Emergency Medicine
Aria	Oncology Prescribing Programme
Badger	Neonatal

System Name	Specialty
Bluespier	Orthopaedics
National Breast Screening System	Breast Care
Integrated Child Health System	Child Health
Choose and Book	Referral management system
CITO	Scanned paper records
CPAD	Pain Clinic
CRIS	Radiology Administrative Information
Day Assessment	Day Assessment
Delayed Discharge System	Not specialty specific
Dendrite	Vascular Medicine
Echo Database	ECG – Cardiology
ESP	Newborn Hearing System
Galaxy	Theatre Management System
Haematology	Haematology
Infection Control	Microbiology
ICT Echo	Intensive Care Medicine
Lantis	Radiotherapy
Maxims	Trust-wide
Medicas Outreach	Intensive care medicine
Medisoft	Ophthalmology
Mellowood	Fertility
NerveCentre	Trust-wide
Neuroworks	Neurophysiology
Novacor	Cardiology

System Name	Specialty
Orion	Diabetic Retinopathy
PAS	Patient Administration System
Proton	Renal Medicine
Scorpio	Endoscopy Medicine
Somerset Cancer Register	Cancer Medicine
Stork	Maternity System
TM Insight	Pharmacy
Tomcat	Cardiology
Viewpoint	Fetal Medicine
WebPACS	Radiology images
Winpath	Pathology
Paper Records	Clinical Oncology. Therapies. Main health record. Child Health. Dietetic records. Mammography.
Complaints and Compliments	Datix. Quanta.

Where incorrect filing has been identified within a patient record it must be recorded using the Trust's Incident Reporting System, Datix, including as much information about the wrong information, who it belongs to and whose records it was found in. The Records Management Team will manage this through Datix.

Where personal identifiable information has been found in inappropriate areas it must be handed into the nearest Reception Desk and reported using the Trust's Incident Reporting System, Datix. The Records Management Team/Information Governance Team will manage this through Datix and will collect the identified information.

Collecting/Sending Information

Individuals and their representatives will be asked wherever possible to collect the copies of their personal information from the department. This will ensure that the information is being given to the person applying for it and provides security of knowledge that confidentiality is being maintained. The person collecting the information will be asked to sign a declaration of their responsibility to keep the information confidential and to dispose of it securely once finished with. Where this is not possible the Trust will send the copies of the clinical information by Special Delivery. The information will be marked “Private and Confidential” and “To be opened by addressee only”, this will ensure that confidentiality is being preserved and the information is being signed for upon delivery.

Dissemination and Implementation

All Trust staff will be made aware of their responsibilities and compliance with policy and specifically, for being able to identify a formal and informal request for access to or disclosure of information through a variety of methods, including (but not limited to):

- Corporate Induction.
- Local induction, specifically for those in Health Records.
- Specific training:
    - Staff working in the Information Governance Office.
- Health Records staff.
- Records Management Leads, but specifically those in the following areas:
    - Human Resources department.
    - Occupational Health department.
    - Finance department.
- Intranet and Internet Records Management Websites.
- Document Library.
- Information Governance Group.
- Health Records Group.
- Patient Administration User Group.

Corporate Induction

All staff new or returning to a new appointment after a period of absence are required to attend the Trust Corporate Induction Programme. Specifically, there is an allocated section on Information Security and Records Management. By attending this Induction, staff will understand their most basic responsibilities in handling information, information security, confidentiality, record keeping and where to direct a request for access to/disclosure of information.

Local Induction

All new staff or returning to a new appointment after a period of absence will be expected to undergo local induction training that will be specific to the department that they will be working in. Any specific requirements relating to records management within the department should be included at this point.

Specific training

Staff working in the Disclosure Office will be expected to follow internal procedures that detail how to deal with access to/disclosure of information. Staff will also be expected to complete the on-line Records Management Training module through the Information Governance website, specifically the module relating to access to health records.

Groups/Committees

The Policy will be approved by the Information Governance Group and circulated amongst the attendees.

The Policy will be circulated to appropriate and relevant staff as part of the consultation process and then once approved tabled for information and circulation to the wider distribution list.

The Policy will be tabled for information and circulated to the staff in the wider health community who handle and manage the Trust's records.

Document Library

Once approved the Policy will be uploaded onto the Trust's Document Library for access by all staff.

Intranet and Internet Records Management Websites

Once approved the Policy will be referenced on the Records Management website.

Monitoring compliance and effectiveness

The database provides the ability to run reports on requests for personal identifiable information, showing how often requests are received, the status of the requests and how many move on to becoming a claim.

Objectives

1. To provide evidence that this policy has been embedded throughout the organisation.

2. To provide evidence of compliance with this policy.

3. Improve the quality of accessing/disclosing personal identifiable information.

4. To identify areas of improvement and document in an action plan.

Scope

a) Number of subject access requests to disclose information.

b) Number of access to health records requests to disclose information.

c) Number of DSS requests to disclose information.

d) Number of insurance requests to disclose information.

e) Number of litigation requests to disclosure information.

f) Number of human resource information requests.

g) Standard of copy records.

h) Number of records exceeding the 30-day deadline of disclosure.

Resources

- These audits are reliant upon a number of staff groups:
  - Information Governance Disclosure staff to collect information.
  - Member of staff to aggregate figures.

Frequency

Reporting will be carried out monthly within the department, culminating in a quarterly and annual report.

Methodology

A template is prepared with dates set for the Disclosure Office to monitor activity once a month for one week.

Reporting:

Information Governance Group:

Information is included in the report to the Information Governance Group.

Care Group Quality Board:

An aggregated report will be tabled at the Care Group Quality Group for dissemination through the Care Groups to ensure that any non-compliance with the policy as highlighted in the audit is actioned.

External Monitoring Bodies:

The following bodies will expect to see the results of these audits as part of the external monitoring process:

- NHS Litigation Authority.
- Data Protection and Security Toolkit.
- Care Quality Commission.

Useful References

The main legislative measures that give rights of access to personal identifiable information include:

- The Access to Health Records Act 1990 - rights of access to deceased patient health records by specified persons - further information can be found on the Information Commissioner's Office website.

- The Medical Reports Act 1988 - right for individuals to have access to reports, relating to themselves – further information can be found on the National Archives website (Access to Medical Reports Act 1998).

- The Freedom of Information Act 2000 gives a right of access to recorded information held by public authorities. The FOI is not intended to gain access to private sensitive information about themselves or other, such as information held in the health record. Further information can be found on the National Archives website (UK Public General Acts).

- Adoption and Children Act 2002 - Further information can be found on the National.

- Archives website (UK Public General Acts).

- Children Act 2004.

- Further information can be found on the National Archives website (UK Public General Acts).

- Care Quality Commission – further information can be found on the Care Quality Commission website.

- Records Management Code of Practice for Health and Social Care 2016, which gives guidelines on using and disclosing patient information – further information can be found at the Department of Health's website.

- Disability Discrimination Act – further information can be found at the Department of Health's website.

- Department of Health Informatics Directorate - Information Governance:

- Information Governance ensures the necessary safeguards for, and appropriate use of patient and personal information. Further information can be found on the NHS Digital website.

- NHS complaints procedure – further information can be found on the NHS website – choice in the NHS, rights, and pledges.

- Complaints to Information Commissioner – further information can be found on the Information Commissioner's website.

- Requesting Amendments to health and social care records – further information can be found on the National Information Governance Board for Health and Social Care website.

- Parental Responsibility – further information can be found on the British Medical Association website. – (consent and capacity).

- Patient health records: access, sharing and confidentiality briefing paper.

This policy has been written in line with the Department of Health Guidance for Access to Health Records Requests dated February 2010. This policy should be read in conjunction with the following and most recent related legislation, National guidance, and Trust policies:

- Information Sharing Protocol.

- Confidentiality: NHS Code of Practice.

- Complaints Policy.

- DPA18.

- UK GDPR.

- Access to Health Records Act 1990.

- The Human Rights Act 1998.

- The Freedom of Information Act 2000.

- The Access to Medical Reports Act 1998.

- Records Management: NHS Codes of Practice for Health and Social Care.

- NHS Information Governance.

- Information Security Policy.

REQUEST FOR ACCESS TO PERSONAL DATA

Under the Data Protection Act 2018 (GDPR)

Please complete in block capitals

Particulars of person whose information is requested		
Title:	Surname:	Date of birth:
Forename(s):		
Current Address:		Telephone Number:
Email Address: **IMPORTANT INFORMATION** Please be advised that your information will be sent by secure electronic file transfer (where possible), the information can then be downloaded. The information will not be sent through e-mail but through Kiteworks, this is a secure mobile file sharing solution and complies with data protection legisaltion.		
If name and/or address was different from above during the period(s) to which the application relates, please give details:		
Previous surname(s):		
Previous address(s):		

INFORMATION REQUIRED –

Please provide as much information as possible of the episode(s) of care you are interested below.

*If you require clinical imaging only please state the type of imaging (MRI, X-ray, CT etc) and the date, if the date is unknown please list the anatomy of the imaging (Knee, Head, Arm etc)

*If you require some but not 'all' of your health records then please detail the specialty (Dermatology, Obstetrics, Audiology etc) or the date range required (April 2012 – November 2016 etc)

INFORMATION REQUIRED	**DATES (if known)**	**HOSPITAL EPISODE/ DEPARTMENT/CONSULTANT**	**TICK THE INFORMATION REQUIRED**
*Clinical imaging only - partial			
Clinical imaging – all	n/a	n/a	
*Health records – partial			
Health records and clinical imaging - all	n/a	n/a	
Attend to view health records			

DECLARATION

I declare that the information given in this form is correct to the best of my knowledge and that

(Please tick were appropriate)

• I am the person named overleaf (**please complete Part 1**)	
• I am acting on behalf of the person named overleaf (**please complete Part 1 and 2**)	
• In the case of a person under the age of 16 I am the parent/legal guardian (**please complete Part 1 and 3**)	

AUTHORISATION

PART 1
Applicant's name:
Address to which a reply should be sent if different from that overleaf:
Signature of applicant: Date:
PART 2
I hereby authorise the Royal Cornwall Hospital NHS Trust to release details of records relating to my treatment as stated overleaf to: Name: Address/e-mail: Signature: Date:
PART 3
In the case of a person under the age of 16, a parent or responsible legal guardian should certify that the child is: • incapable of understanding the request **OR** • has consented to making the request
Name of parent/legal guardian:
Address if different from that overleaf:
Signature: Date:

The appointed Data Protection Officer for the Royal Cornwall Hospitals Trust is:

Mr Mark Scallan. PC.dp. PC.foi

Please return this form to: - Disclosure Office, Kedhlow Building, Royal Cornwall, Hospitals NHS Trust, Truro, Cornwall TR1 3LJ or e-mail: rch-tr.Disclosure@nhs.net

DECLARATION

The Access to Health Records Act 1990 and the Common Law protects the confidentiality of patients even after they have died.

For this reason, deceased patient's records can only be disclosed in limited circumstances.

Where a patient has died the Trust may only disclose copies of the deceased patient's medical records to:-

a) The deceased patient's personal representative who may have a claim arising out of the deceased patient's death.

OR

b) Any person who may have a claim arising from the death.

Only records that are relevant to any claim arising out of the patient's death may be disclosed in either of these classes.

If you are the personal representative of the late (please insert full name) …… the Trust requires either:-

- A grant of probate confirming this **(in the case of an executor)**;
- A grant of letters of administration **(in the case of an administrator)**;
- **(in either case)** A copy of your solicitor's letter confirming your entitlement as personal representative of the estate;
- Evidence that supports there is a claim on-going, (legal documentation, a copy of your solicitors letter)

Royal Cornwall Hospitals NHS Trust is also required to know in what circumstances you consider you have a claim relating to your late husband/wife/partner/relative's death (please circle the appropriate answer), as we can only disclose records relevant to this claim. If you are not the personal representative and/or do not have a claim arising from the deceased, then the Trust will be unable to disclose copies of the medical records.

I declare that the information given in this form is correct to the best of my knowledge and that:

- I am the person named overleaf (Part 1)
- I am acting on behalf of the person named overleaf (Part 1 and 2)
- I have a claim arising from the patient's death and wish to access information relevant to my claim (Part 1 and 3) *In this instance a separate covering letter will be required giving an explanation of the claim being considered*

If you are acting on behalf of another person, Part 2 of the 'Authorisation' section below must be completed.

PART 1
Applicant's name
Address
Email Address ***(for correspondence only – we will not send records via email)*** Can we contact you via email? Yes/No (please circle) Telephone Number Home Mobile Number
Relationship to patient
I agree to pay the standard charges of up to £50 and note that I will be contacted if the application exceeds this amount Signature of applicant Date
PART 2
I hereby authorise the Royal Cornwall Hospitals NHS Trust to release details of records relating to the treatment of the patient named overleaf to: …… To whom I have given my consent to act on my behalf and I confirm I am the deceased's personal representative. Signature Date
PART 3
I can confirm that I have a claim arising from the patient's death; the details of my claim are detailed in a covering letter. Signature Date

Please return this form to: - Disclosure Office, Kedhlow Building, Royal Cornwall Hospitals NHS Trust, Truro, Cornwall TR1 3LJ or e-mail: rch-tr.Disclosure@nhs.net

The appointed Data Protection Officer for the Royal Cornwall Hospitals Trust is:

Mr Mark Scallan. PC.dp. PC.foi

Charges relating to the Disclosure of Personal Information

Information Disclosed Under the Access to Health Records Act

Disclosure of these records relate specifically to deceased individuals.

A charge of £10 will be made in respect of each request made unless an entry has been made in the 40 days prior to the request. There will also be a charge of 30p per side of information copied. Package and posting are not included in these charges.

Where package and posting are charged separately this will be dependent on the weight of the information being sent and has been based upon the “Pricing made easy” document issued by the Royal Mail, for Special Delivery.

Reduced Charges

In those cases where applicants claim financial hardship and are unable to pay the full amount, the matter should be referred to the Data Protection Officer/Records Services Manager; either has the sole discretion to either waive or agree a reduced sum.

The decision to waive or reduce the charge should be based upon an assessment of the applicant’s financial status and evidence of this may be asked for. This may be:

- An Awards Letter for people claiming Income Support.
- An Awards Letter for people claiming Guaranteed Pension Credits.
- An Awards Letter for people claiming Job Seekers Allowance.
- A white card for people who hold an NHS Exemption Certificate.
- An Awards Certificate for people holding a HC2 or HC3 Certificate.

The Records Services Manager/Data Protection Officer also has discretion to waive charges in exceptional circumstances of sensitivity.

Appendix 8. Access to Electronic Systems

User Password/Passcode/Smartcards

All new users will be briefed on the importance of passwords/ passcodes/ Smartcards and instructed in the manner in which they are to be used and protected.

Passwords/passcodes/smartcards must always be treated as though they are classified at the level of the most sensitive data held on the system to which they allow access.

Passwords/passcodes will not be displayed on screens as they are entered and must be held on computer systems in one-way encrypted form.

Where temporary passwords/passcodes are known to the systems administrator or network manager, the user must change the password/PIN immediately on receipt.

Where a temporary password/passcode is defined for an authorised user, e.g. a trouble shooting session, this will be deleted at the end of the session.

Individual passwords/passcodes will not under any circumstances be made known to other members of staff.

User passwords/passcodes should be self-selected by the user and individual. User to be advised that when they type in their password/ passcode to ensure they are not being overlooked by other people.

User passwords/passcode undergo triviality checks, this will ensure the password doesn't relate to the user or the system being accessed.

Passwords are forced to change every 90 days. (some legacy systems do not have a forced change function, so for these systems a manual reminder will be required.) There is a minimum password length of 6 characters (where legacy systems permit). A history is kept of previous passwords for one year so the user cannot reuse that password. Looking to the future the National Cyber Unit is recommending passwords of 15 characters and these are never refreshed as they would be considered too complicated to hack. The Trust should be ensuring all new systems procured are able to conform to this standard.

Privileged accounts should have their passwords changed every 30 days.

Passwords should be stored separate from the application system data, in encrypted format and the Vendors default passwords changed immediately after installation.

Staff Changes should have their accounts locked, not deleted, so any system usage and data controlled by that user can be tracked.

Monitoring System Access and Use

There will be established procedures authorised by management for monitoring system use and a process for the management of system alerts where access was unusual or inappropriate.

System audit trails including all recorded security related events will be produced and kept indefinitely pending national guidance.

Areas to be considered are:

- Access failures.
- Review of log-on patterns for indications of abnormal use or revived user-IDs.
- Allocation and use of accounts with a privileged access capability.
- Tracking of selected transactions.
- The use of sensitive resources.

Application Access Control

Some legacy systems will not be able to support these measures; an exception will be made where this is the case.

Information access restriction (Role Based Access, Legitimate Relationships and Audit Alerts) - Access to data will be granted only to staff that need to use the data to perform their job function not exceeding an agreed level of detail required and will be further restricted to enable access to personal data only where a legitimate relationship exists between the user and the subject.

This also applies to security data that will be accessed only by security or appropriately authorised Information Governance (IG) staff or Information Asset Owners.

When and if data access rights are changed or bypassed a report will be produced showing:

- The identity of the person making the change.
- The authority for the change.
- What is being changed.
- Who would or could be affected by the change.
- The date and time of the change.

Only in emergencies may staff be granted access to live data over and above the access originally assigned by the user sponsor, and the Information Asset Owner should be informed.

Where emergency access rights are granted (e.g. to technical support staff or engineers) this will be done under a specially allocated user-ID and be password controlled. The password will be changed on completion of the emergency. All emergency activity will be monitored and controlled by logs and audit trails.

All detected unauthorised attempts to access systems or data must be reported immediately to the IT security officer as a security incident and the Information Asset Owner should be informed. In future, when Sealed Envelopes are introduced, any unauthorised attempts to access this type of information must be reported to appropriately authorised IG staff carrying out a devolved Caldicott function.

All systems or stand-alone databases containing personal identifiable data (staff or patient) will be registered with the IG Department for Data Protection Act compliance and Caldicott standards review purposes.

Appendix 9. Data Quality

Data held in Trust computer systems must be "fit for purpose".

All staff must be trained to ‘Get it Right First Time’ (GIRFT). This is first and foremost a patient safety requirement, a data protection issue if the Trust is not holding accurate and up-to-date information and it will reduce the need for back-office support to correct information before it is reported upon, allowing other important work to be focussed on.

All data will be routinely tested, and regular reports made available on its quality.

Standards for Trust data quality must meet Data Security and Protection Toolkit requirements.

Failure to comply with the Trust’s procedures may result in the removal of access from information systems.

Without approved training, no passwords will be allocated enabling access to any systems no matter the status of the member of staff.

Regular audits of clinical coding will be undertaken to validate clinical information.

It had been agreed that no updates would be made to the demographic details of patients from information provided and available on the NCRS National Care Records Service. This decision was based on the known accuracy of the Trust’s Referral Index (RI) which is considered to have a greater degree of accuracy due to the work carried out by the Trust’s Data Quality Team. There have been many instances where the data held on the Spine has been proven to be of poor quality when compared to that of the RI. The risk of keeping the data held locally as true was deemed to be less than that of using the NCRS National Care Records Service. This decision was made in consultation between the Trust’s Records Services Manager, the Trust’s Data Protection Officer, and the System Application Support Manager. The process for tracing patients against the NCRS National Care Records Service has been reviewed in preparation for the eCare programme. It has been decided that this process can restart as the demographic details are not automatically being updated. All patient records will need to be traced prior to ‘go live’ of eCare. The Data Quality Team are running this process weekly and have a report of any discrepancies between the data, this is investigated and updated as necessary.

Failure to Maintain Data Quality

All instances of failure to maintain adequate data quality in Trusts systems (for example, by entering incorrect data) will be dealt with as follows:

- First Instance – The individual responsible for the data quality failure will be contacted to inform them of the error and will be offered further training.

- Second Instance – The individual responsible for the data quality failure and their Line Manager will be contacted to inform them of the error and the individual will be offered further training.

- Third Instance – The individual responsible for the data quality failure and their Line Manager will be contacted to inform them of the error. Access to the relevant information system will be removed from the individual concerned until they have successfully completed further training.

- Fourth and Subsequent Instances – The individual responsible for the data quality failure and their Care Group Manager will be contacted to inform them of the error. The Care Group Manager will be expected to consider initiating the Trust's Capability Procedure to deal with the inability of the individual to maintain adequate data quality.

Dissemination and Implementation

Corporate patient activity information will be posted on the Trust intranet.

The Trust has developed and maintained suitable training courses for appropriate staff to increase awareness of the requirement for accurate data and to undertake the procedures necessary to achieve this.

Staff must attend appropriate training to ensure an adequate level of competency in the patient administration functions used in their role.

The Data Quality function will monitor activity and report any perceived weakness of staff data input to the appropriate line manager and IAO.

The annual cycle of the mandatory training programme will ensure all staff understand the significance of their information duties and how others use data.

Monitoring compliance and effectiveness

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	All systems containing data – initially first 10 patients critical systems then followed by another 10 systems which will include corporate systems. Data will be routinely tested, and regular reports made available on the quality metrics.
Lead	The has responsibility for the analysis of Data Quality for the Trust. This will be supported by the Data Quality Team.
Tool	Data will be routinely tested, and regular reports made available through the Information Governance Group Regular validation processes will be undertaken on data to assess its accuracy, e.g., waiting list validations, checks for logical errors, duplicate records, Completeness and Validity checks within all clinical systems. Accredited external sources of information e.g., NCRS will be used to assist with the validation of patient records. Accredited external sources of information will be used to assist with the validation of corporate records.

Information Category	Detail of process and methodology for monitoring compliance
	The Trust will submit extracts to the NHS-wide Secondary Use Service (SUS) which holds comparisons against the national average % and other Trusts. See example below. Data identified in the Trust's electronic systems will be monitored through the Data Quality Dashboard. See example below.
Frequency	Data held within the PAS system will be monitored daily by the Data Quality Team. Monthly reports of the RCHT Data Quality dashboard will be submitted to the DQAG. Bi-monthly reports of the SUS Data Quality dashboard will be produced and submitted to the IGG.
Reporting arrangements	Information Services Department will provide regular performance updates of data efficiency and collection through regular reports for patient-based systems. These will be based on the Data Quality Dashboard reports which cover IP, OP, Maternity, ED, and Data Quality Indicators. This will be provided at the DQAG and IGG where appropriate. This will be achieved through using external tools, e.g., SUS Data Quality Dashboard. The RCHT Data Quality Dashboard will be reviewed by the DQAC on a bi-monthly basis. Actions identified by the above boards will identify areas of concern and these will be documented in the minutes for the appropriate meeting. The Trust Board will receive assurance on data quality through the Trust's Integrated Governance and Assurance Framework.
Acting on recommendations and Lead(s)	The IGG or DQAG will recommend areas for evaluation when identified from the dashboard data. Performance data will be passed to Care Groups as required for action. Any additional requests for information and reports will be passed to the Information Services Department.
Change in practice and lessons to be shared	Required changes to practice will be identified and actioned within 2 weeks. The relevant IAO will be identified to take each change forward where appropriate. Lessons will be shared with all the relevant stakeholders. Training will be provided and targeted in response to recurring data quality issues.

Example of Data Quality Dashboard Reporting Tool

Data Quality Dashboard - 2023/24

Summary Sheet

		April	May	June	July	August	September	October	November	December	January	February	March
CLINICAL	PAS BI	Y	Y	Y	Y	Y	Y						
	Clinical Coding	Y	Y	Y	Y								
	PAS Booked Elective Admissions	G	G	G	G	G	G	G	G				
	HR Notes Tracing												
	PAS Inpatients & RTBM	A	R	A	R	R	A	A	A				
	PAS Outpatients	G	G	G	G	G	G	G	G				
	Electronic Patient Record	A	A	A	A	R	A	Y	Y				
	Clinical Imaging	G	G	G	G	G	G	G	G				
	Theatres	G	G	G	G	G	G	G	G				
	Pathology	A	A	A	A	A	A	A	A				
	Paper Health Record												
	Pharmacy	G	G	G	G	G	G	G	G				
	Maternity	A	A	A	A	A	Y	Y	Y				
	Oceano	G	G	G	G	G	G	G	G				
	Badger	G	G	G	G	G	G	G	G				
	Cardiology												
	Capture Stroke												
	eNotes	A	A	A	A	A	A	R	R				
	Medisoft												
	Scorpio												
	Aria												
	Nervecentre												
	Orthopaedics												
	ICE												
CORPORATE	ESR Payroll												
	Healthroster	A	A	A	A	A	A	A	A				
	Unit 4												
	Document Library	R	A	A	A	R	R	R	R				

Example of SUS Data Quality Reporting Tools

SUS DQ DASHBOARD SUMMARY 20-21
monthly monitoring

Patient Category	Category	Aug-20 RCHT %	National %	Sep-20 RCHT %	National %
DQ DASHBOARD					
APC	Commissioner	100.0	94.6	100.0	95.1
	HRG4	98.5	96.6	97.8	96.2
	NHS Number	99.8	99.5	99.8	99.6
	Org of Residence	99.8	99.7	99.8	99.7
	Patient Pathway	90.7	64.9	91.1	65.9
	Postcode	99.9	99.9	99.9	99.9
	Reg GP Practice	100.0	99.8	100.0	99.8
	Site of Treatment	100.0	97.7	100.0	97.4
OP	Commissioner	100.0	92.5	100.0	93.1
	HRG4	100.0	99.3	100.0	99.3
	NHS Number	99.9	99.7	99.9	99.7
	Patient Pathway	62.5	67.2	62.2	67.1
	PostCode	99.9	99.9	99.9	99.9
	Referral Received date	28.6	95.4	28.8	95.4
	Reg GP Practice	100.0	99.8	100.0	99.7
	Site of Treatment	100.0	97.2	100.0	99.9
ED	Commissioner	92.1	88.7	92.0	90.1
	Ethnic Category	95.1	92.4	94.9	92.5
	NHS Number	98.9	97.9	99.9	98
	Postcode	99.9	99.3	99.9	99.3
	Reg GP Practice	99.9	98.8	99.9	98.9
	Org of residence	99.9	96.8	99.9	96.8
	First investigation	47.3	70.6	47.5	70.5
	First treatment	94	80.1	94	80
MATERNITY					
BIRTH 120					
	Commissioner	100.0	96.3	100.0	96.9
	Birth weight	99.2	87.6	99.4	87.2
	Ethnic Category	100.0	97.2	100.0	97.2
	HRG4	98.7	94.4	98.6	94.2
	Int place of delivery	99.5	74.8	99.5	74.4
	NHS Number	100.0	99.6	100.0	99.6

SUS DQ DASHBOARD SUMMARY 22-23

Monthly Monitoring

Patient Categor	Categor	M5 Apr 2023 to Sep 23 RCHT %	National %	M6 Apr 2023 to Oct 23 RCHT %	National %
DQ DASHBOARD					
APC	Commissioner	100.0	99.2	100.0	99.2
	NHS Number	99.8	99.6	99.8	99.6
	Org of Residence	99.7	96.2	99.7	96.3
	Patient Pathway	89.7	70.2	90.4	69.5
	NHS No Status Indicator	99.5	99.7	99.5	99.7
	Postcode	99.9	99.9	99.9	99.9
	Reg GP Practice	100.0	99.8	100.0	99.8
	Site of Treatment	100.0	97.1	100.0	97.1
	Ethnic Category	100.0	94.7	100.0	94.7
OP	Commissioner	100.0	98.5	100.0	98.6
	NHS Number	100.0	99.8	100.0	99.8
	NHS No Status Indicator	99.9	99.9	99.9	99.9
	Patient Pathway	60.1	67.6	60.7	97
	PostCode	99.9	99.9	99.9	99.9
	Referral Received date	36.4	94.1	36.5	94.1
	Reg GP Practice	99.7	99.6	99.7	99.5
	Site of Treatment	99.9	96.2	99.9	96.2
	Ethnic Category	99.9	91.5	99.9	91.5

		Apr 2023 to Sep 23 RCHT %	National %	Apr 2023 to Oct 23 RCHT %	National %
ECDS	Commissioner	100	95.6	100	95.8
	Ethnic Category	91.8	95.9	92.5	92.2
	NHS Number	96.7	96.2	97.3	96.6
	Postcode	28.0	96.8	27.0	96.6
	Reg GP Practice	99.9	98.8	99.9	98.7
	Clinical Investigation (SCT) - First	46.7	66.9	49.4	74.1
	Procedure (SCT) - First	93.6	78	93.6	78.2
	Procedure Date- First	93.5	69.4	93.4	69.2
	Procedure Time - First	14.3	49.3	14.6	49.3
	Discharge Follow-up (SCT)	99.7	73.7	99.7	72
	Discharge Info Given (SCT)	44.1	7	44	6.8
	Activity Service Request Time	99.9	97.4	99.9	97.5
	Ambulance Call Identifier	85.5	84.7	87.1	83.4
	Time Seen for Treatment	100	87.9	100	87.2
	Clinically Ready to Proceed			100	50.1
	Injury Intent (SCT)	100	41.6	99.9	41.5
	Initial Assessment Time	99.9	90.7	99.8	90.9
	Injury activity status	0.2	17.5	0.2	17.1
	Injury activity type	0.1	17.5	0.2	17.1
	Injury Alcohol or Drug Invol				
	Injury Date	100	60.4	99.9	60.3
	Injury Time	96.5	51.1	86.1	51.6
	Injury Mechanism	100	25.4	99.9	25.4
	Place of injury	0.2	23.2	0.2	22.7
	Overseas visitor charging	36.9	43.6	46.9	43.2
	Acuity	99.2	89	99.3	88.1
	Treatment Function (DTA)	15.1	12.4	99	51.1