Trust Policy	

Health Records Policy

Issue Date	Review Date	Version
August 2020	August 2023	5.0

Purpose

To ensure that health records management, both paper and electronic, comply with regulatory and operational requirements.

Who should read this document?

All staff who handle the paper health record and/or view and amend electronic health records.

Key messages

This document details Trust policy on the completion, use, tracking, storage, retrieval, archiving and disposal of health records and details the responsibilities of all users to ensure that all records are:

- secure
- retained and disposed of appropriately
- available when needed
- can be interpreted
- can be trusted
- can be appropriately maintained through time

Accountabilities

Owner	Central Records Library Manager (Governance)
Review	Health Records Steering Group (HRSG)
Ratification	Director of IM&T (Chief Information Officer)
Dissemination (Raising Awareness)	Head of Health Records
Compliance	Head of Health Records

Links to other policies and procedures

Clinical Records Keeping Policy
Information Governance Policy
Management of Freedom of Information Requests SOP
Data Protection SOP
Subject Access Request (SAR) Policy
System Level Security Policies
Managing Health Records SOP
For a list of Health Records APNs see Managing Health Records SOP

Version History

Draft 1.2	April 2011	1st Draft – Associate Director of Patient Administration.

Draft 1.2	May 2011	2nd Draft – Records Services Manager
1.2	June 2011	Approved by the Paper Records Transformation Group
1.3	Feb 2012	Reviewed and amended by Records Services Manager
2.1	May 2012	Reviewed by Records Services Manager
3	April 2015	Reviewed and amended by Head of Health Records and eNotes Implementation to include changed roles, reference to the Records Management Code of Practice Review and to the eNotes Programme.
3	April 2015	Ratified by the Director of Planning & Site Services
3	April 2015	Approved by the Paper Records Transformation Group
4	April 2016	Reviewed by Central Records Library Manager
4.1	December 2018	Extended to March 2019
4.2	April 2019	Extended to July 2019
4.3	September 2019	Extended to September 2019
4.4	November 2019	Extended to December 2019
4.5	June 2020	Extended to August 2020
5.0	August 2020	New Policy to supersede Version 4.5 of the Health Records Policy. This is a complete rewrite to include full reference to Electronic Health Records.

PHNT is committed to creating a fully inclusive and accessible service.

Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff.

We will treat people with dignity and respect, actively promote equality and diversity, and eliminate all forms of discrimination regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/ maternity.

An electronic version of this document is available on the Trust Documents. Larger text, Braille and Audio versions can be made available upon request.

1 Introduction

UK Data Protection legislation comprises the UK Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR). The Trust has a duty under DPA 2018 to ensure that there is a valid legal basis to process personal and sensitive data. As an NHS hospital the Trust has been authorised by the government to provide healthcare and as such must keep accurate records of patients care. Under GDPR our legal basis for holding this information is Article 6(1) (e) and 9(2) (h).

The DPA 2018 covers how the Trust obtains, holds, records, uses and stores all personal and special category (e.g. Health) information in a secure and confidential manner. This Act covers all data and information whether held electronically or on paper and extends to databases, videos and other automated media about living individuals including but not limited to Human Resources and payroll records, medical records, other manual files, microfilm/fiche, pathology results, images and other sensitive data. DPA 2018 is applicable to all staff; this includes those working as contractors and providers of services.

For more information about your obligations under the DPA 2018 please see the Data Protection Policy, in the Document Library G:\DocumentLibrary\UHPT Trust Documents or contact the Information Governance Team informationgovernancepht@nhs.net Records Managers are expected to adhere to the DPA 2018 in regard to managing records.

The DPA 2018 has 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.

Information and Record 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. Documents and archives, including those held within electronic systems, are also recorded information and encompassed by the discipline of information and record 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 University Hospitals Plymouth NHS Trust (UHP) 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.

Personal Identifiable data (PID) in health records must be managed in accordance with this policy and commensurate with current legislation, clinical and operational needs, this includes photography, images and recordings.

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 2016 and also upon current legal requirements and professional best practice.

The Records Management Code of Practice for Health and Social Care 2016 sets out what people working with or in NHS organisations in England need to do to manage records correctly. It is based on current legal requirements and professional best practice and was published on 20 July 2016 by the Information Governance Alliance (IGA). www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

Appendix 3 of the Code contains detailed retention schedules. It sets out how long records should be retained, either due to their ongoing administrative value or as a result of statutory requirement.

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.

Accurate, up to date and accessible information is essential to the planning and delivery of high quality patient care and therefore effective records management is vital.

All NHS staff have a responsibility to manage health records in line with this policy, from the creation of a record to its ultimate disposal.

2 Purpose

The purpose of this policy is to establish a framework for the Trust to ensure it manages its health records effectively. It will confirm that procedures are in place for the creation, use, tracking, retrieval, storage, 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.

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 and any successor statutory regulations and standards:

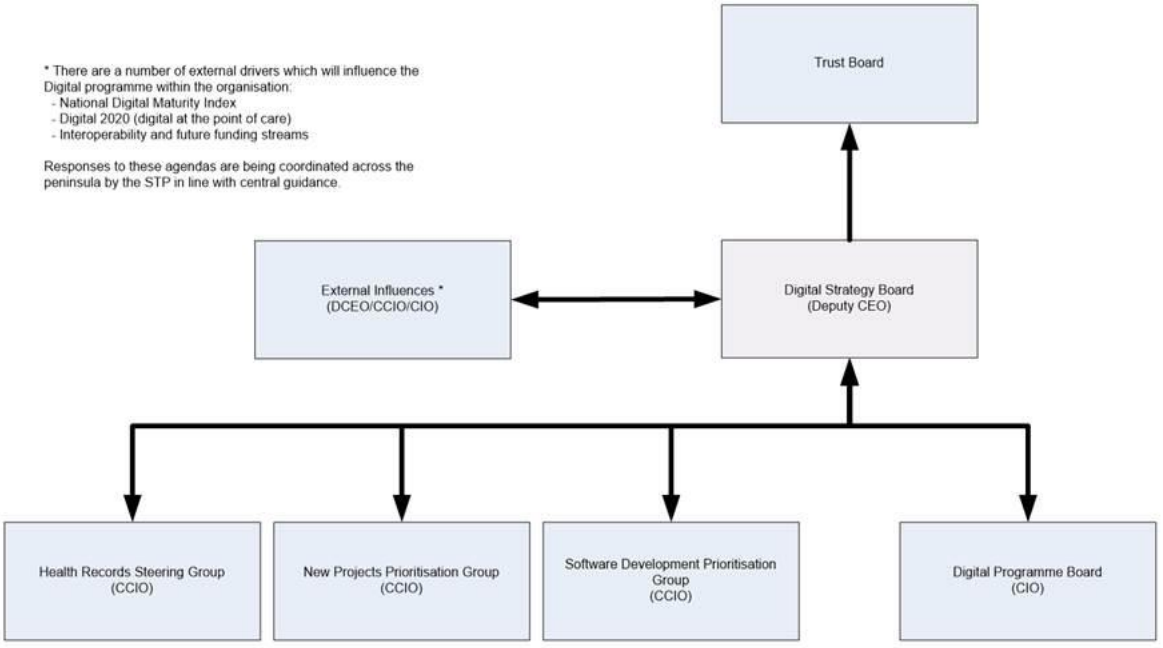
- Public Records Act 1958
- DPA 2018
- Freedom of Information Act 2000 with particular focus on the Lord Chancellor's Code of Practice on the Management of Records under Freedom of Information
- Environmental Information Regulations 2004
- Limitations Act 1980
- Common Law Duty of Confidentiality
- NHS Confidentiality Code of Practice
- Records Management Code of Practice for Health and Social Care 2016
- Care Quality Commission Declaration
- Data Security and Protection Toolkit requirements
- NHS Litigation Authority Standards (NHSLA) [1]

[1] NHSLA Records Standards. Whilst these standards continue to reflect good practice they are no longer updated or monitored by the NHSLA.

- British Standards ISO 27001 Information Security Management (was BS7799)
- British Standards ISO 9001Quality management systems

The Trust is committed to ensuring that all relevant information is provided at the point of patient care and that the information is of a high standard, remains confidential and secure. Health records should provide an accurate, legible and contemporaneous record of patient care.

The Digital Strategy Board (DSB) on behalf of the Health Records Steering Group (HRSG) has adopted this Health Records Policy on behalf of the Trust Board. The Chief Clinical Information Officer (CCIO) is the chair of the HRSG and also sits on the DSB with both the Director of IM&T (Chief Information Officer) and the Deputy Chief Executive who is a Trust Board Member. See below:



This Policy aims to deliver standardised ways of working and a number of organisational benefits:

- Clear standards to manage health records
- Improved structure and quality of the content of health 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
- Improved physical and electronic storage of information
- An informed, educated and competent workforce
- Improved use of staff time

The information within a health 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.

Managing the way in which staff handles 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. Please see the Trusts Audio and Visual Recording Policy. G:\DocumentLibrary\UHPT Trust Documents\Information Governance\Audio and Visual Recording Policy.pdf

Standards specifically relating to the content of health records in case notes are detailed within the **Clinical Record Keeping Policy.** G:\DocumentLibrary\UHPT Trust Documents\Clinical Records Management\Clinical Records Keeping Policy.pdf

3 Scope

This Policy applies to all NHS health records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector or other health care providers, regardless of the media on which they are held. This includes any records held either electronically or in a paper format.

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 businesses. The DPA 2018 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'. (See also The British Medical Association (BMA) definition of a Health Record p9).

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

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
- 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)

Format:

- Photographs, slides and other images
- Microfilm
- Audio and video tapes, cassettes, CD-ROM
- 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

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 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
- Archiving
- Disposal
- Disaster Planning/business continuity

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 health 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.

Photography and recordings and specifically recordings made:

- On healthcare premises within or outside of the UK (including Theatres)
- As part of the assessment, investigation or treatment of patients' conditions or illness and may include video links in Theatres
- 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'

Please see the **Trusts Audio and Visual Recording Policy.** Available on the network share (drive) G:\DocumentLibrary\UHPT Trust Documents\Information Governance\Audio and Visual Recording Policy.pdf

4 Definitions/Glossary of Terms

Administrative Procedure Notes (APN's) - are a series of procedural documents that detail the way staff should carry out certain duties. The APN's, referred to, throughout this policy, are available to all staff via Trust Documents on the network share (drive). \\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs

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.

Disaster recovery – The ability of an organisation to respond to a natural or manmade catastrophic event, so that it can continue to function. Disaster recovery is a sub-set of

business continuity which is primarily focussed on the IT aspects of the organisations 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.

Health Record (Medical Record)
The Data Protection Act 2018, describes the Health Record as "consisting of information about the physical and mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual". The health record is the Trusts main acute record and is also referred to as 'a hospital record', 'patient case note', 'patient record', or 'patient notes'.

The British Medical Association (BMA) defines a **Health Record** as:
'Any record which consists of information relating to the physical or mental health or condition of an individual made by a health professional in connection with the care of that individual. It can be recorded in a computerised form, in a manual form or a mixture of both. Information covers expression of opinion about individuals as well as fact. Health records may include notes made during consultations, correspondence between health professionals such as referral and discharge letters, results of tests and their interpretation, X-ray films, videotapes, audiotapes, photographs, and tissue samples taken for diagnostic purposes. They may also include internal memoranda, reports written for third parties such as insurance companies, as well as theatre lists, booking-in registers and clinical audit data, if the patient is identifiable from these'.[2]

For the purposes of this policy the BMA definition above has been adopted.

Information held in the following systems (but not restricted to) will be considered to be a part of the patient record.

- Patient Administration System (iPM)
- EDIS
- PACS
- iCM
- SALUS
- Medisoft
- Infoflex
- Electronic Renal Patient Service
- Physical Health Record

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

Information Asset - is a system that holds data, both, demographic and activity. For the purposes of this policy these systems are the Trusts critical systems (but not limited to):

- Patient Administration System (iPM)
- EDIS
- PACS

[2] BMA Access to Health Records Guidance for health professionals in the United Kingdom. August 2014

- iCM
- SALUS
- Medisoft
- Infoflex
- Electronic Renal Patient Service
- Physical Health Record
- SeeEHR

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.

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 in Speech and Language Therapy 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.

Records Management - This is the process by which an organisation manages records in any format or media type, from their creation to their eventual disposal. The key components of records management are:

- record creation
- record accuracy
- record keeping
- record maintenance (including tracking of record movements)
- access and disclosure
- closure and transfer
- appraisal
- archiving
- disposal

Subject Access Request (SAR) - This is a request from an individual or an organisation asking that the Trust provides them with the information, relating to an individual, which is held or processed by the Trust. These are normally requests for Medical or Staff

Personnel Records held by the Trust on a patient or staff member by the individual or by their personal representative or solicitor.

System Level Security Policies (SLSP) - These are documents that detail the technical and operational Information governance components of the various key electronic patient record held by the Trust. These documents are maintained and held by the respective System Managers.

Temporary Records (temporary case notes) - These are records that are used whilst the main hospital notes are unavailable and should be amalgamated with the main hospital notes as soon as possible. Please see Trusts Managing Temporary case notes APN. \\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs

5 Ownership and Responsibilities

As health 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.

Role of the Chief Executive
The Chief Executive has overall responsibility for records and information management in the Trust and for ensuring that the Trust meets compliance requirements. This role has 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 Deputy Chief Executive.

Role of the Deputy Chief Executive
The Deputy Chief Executive has delegated responsibility ensuring that the Trust meets its legal responsibility in the management of records and information. They are responsible for the operational delivery of the Health Records Service which has been devolved to the Director of IM&T (CIO) to deliver operationally.

Role of the Medical Director
The Medical Director has operational responsibility for clinical record keeping standards for the consultant/doctor body of staff, delegated via the Assistant Medical Director for Quality and Safety.

Role of the Chief Nurse
The Chief Nurse has operational responsibility for clinical record keeping standards for nursing, midwifery and allied health professionals.

Role of the Senior Information Risk Owner (SIRO)
The Director of Corporate Business is responsible for Information Governance arrangements and as such is the Senior Information Risk Owner (SIRO). As SIRO they will:

- take ownership of the organisation's information risk policy
- act as advocate for information risk on the Board

Role of the Caldicott Guardian

The Caldicott Guardian has responsibility for ensuring that each patient focussed system has appropriate control to support patient confidentiality. They have a particular responsibility for reflecting patients and staff interests regarding the use of personal data and for ensuring personal identifiable data is stored and shared in an appropriate and secure manner.

The framework for appropriate information sharing is set out by the seven principles in the Caldicott Report (2016).

Role of the Data Protection Officer (DPO)
DPOs assist an organisation with monitoring internal compliance, inform and advise on data protection obligations and provide expert knowledge of data protection law and practices. Responsible for Data Protection incident management and acts as a contact point for data subjects and the Information Commissioner's Office (ICO).

Role of the Director of IM&T (CIO)
Reports directly to the Deputy Chief Executive and is responsible for ensuring that the strategic plan for records management is adopted and that appropriate mechanisms are in place. Delegated responsibility for the operational delivery of the Health Records Service. The Head of Health Records reports directly to the Director of IM&T (CIO).

Role of the Head of Health Records
Responsible for:

- Delivery of the operational Health Records Service across the Trust
- Developing health records policies and procedures for case notes
- Coordinating audit activity relating to health records management of case notes in conjunction with Service Line Managers
- Providing assurance in relation to the CQC Records Standards to the HRSG and Caldicott and Information Governance Assurance Committee (CIGAC)
- Compliance with this policy

Role of the CRL Manager (Governance)
Accountable and responsible for the Governance and Assurance processes of the UHP Health Records Service, providing direct support and cover for the Head of Health Records as required.

Role of the CRL Manager (Operations)
Accountable and responsible for the operational management of the UHP Health Records Library Service, ensuring that an efficient, secure and confidential medical records service is available across the Trust and that paper health records are available/accessible when required.

Role of Central Records Library (CRL) Staff
CRL staff support departments with the retrieval, storage and re-filing of the health record but are not responsible for the security, maintenance (including filing into the records) and completeness of the record whilst outside of the CRL. CRL staff will ensure that records stored within the CRL facility are traced and filed appropriately, are available when needed and dispatched in a timely manner to avoid undue delay to the assessment of patient needs by health professionals.

Role of all Service Line Managers and Heads of Department

Are responsible for promoting health records management and ensuring there are operational systems in place within their teams to fulfil the requirements of this policy. This includes ensuring staff receive appropriate training in the management of health records. Also responsible for developing, implementing and monitoring any action plans required as a result of spot-checks and audits on wards and in departments and feeding back all actions to the HRSG.

Role of the Clinical Systems Manager
Responsible for providing the HRSG with biannual reviews of Double registrations and mixed patient records.

Role of the Disclosure Team
Responsible for all subject access and access to medical records requests both from data subjects and solicitors.

Role of the Data Quality (DQ) (Performance Information Team)
Responsible for reviewing and monitoring the quality of information regarding the creation, accuracy and management of electronic records on the Trust's Patient Information System (iPM), using the suite of DQ Reports. These reports are discussed at a monthly Data Quality Steering Group and the action plan relating to compliance and effectiveness is managed monthly by this Group. Reports are discussed and major issues are escalated via the CIGAC.

Role of Information Asset Owners (IAO)
These are senior individuals who understand/address risks of assets they own (usually a Service Line Manager is the IAO for key assets in their service line). They should be aware of what information is held and why within the information assets (electronic systems) under their responsibility.

Role of System Managers/Information Asset Administrators (IAA)
Assists the IAO with the day to day management of an asset. Ensures that procedures are followed (usually the System Manager to a key asset who reports risks up to the IAO). Responsible for detailing the governance of electronic systems in the System Level Security Policies.

Role of individual Staff
All staff who handle records have a duty to:

- Protect patient confidentiality and records security
- Take all reasonable precautions to ensure that the records entered are accurate
- Ensure that notes in their care are in a good physical condition, ensuring that the folder is robust and that all relevant documentation is filed securely within the record
- Ensure that records held within their department are traced and filed appropriately, are available when needed and dispatched in a timely manner to avoid undue delay to the assessment of patient needs by health professionals
- Report records / information related incidents on the Datix System

Role of the Health Records Steering Group (HRSG)
Reporting into the Digital Strategy Board (DSB), the HRSG supports the University Hospitals Plymouth NHS Trust (UHP) in its implementation of an effective management

system for Health Records and Information, in line with the principles contained in the *Records Management Code of Practice for Health and Social Care, 2016*.

The HRSG comprises senior representatives from Medical, Nursing and other allied health professions across the organisation, to promote a holistic approach to health records management.

The HRSG oversees the development of internal and national best practices which are acceptable, practical, owned and supported across the organisation. It also influences the integration and inclusion of health records management standards with other governance, strategies, work programmes and projects e.g. IM&T programmes.

Role of the Caldicott and Information Governance Assurance Committee (CIGAC)
CIGAC is responsible for providing oversight of the Trust's Information Governance and Caldicott responsibilities and to give assurance to the Trust Board that the appropriate arrangements are in place to meet legal, regulatory and best practice requirements.

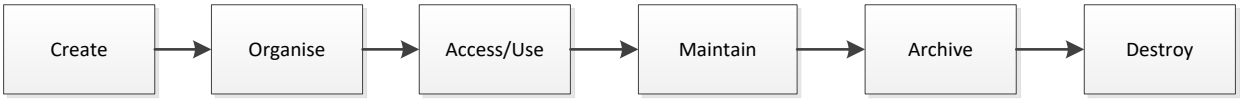
Role of the Digital Strategy Board (DSB)
The DSB, reporting into the Trust Board is the group responsible for:

- Defining the Trust's Digital Strategy and Digital Clinical Strategy
- Defining the Trust's Digital Tactical Plan (1-3 years) to meet interim operational needs
- Approving the commissioning of new tactical projects and agreeing the prioritisation against the Digital Tactical Plan
- Provides the clinical expertise to advise the Trust on all clinical matters in support of the Digital Strategy and digital clinical solutions
- Provides Digital and functional expertise in support of the Digital Strategy and digital clinical solutions

6 Common Standards and Practices

There are a number of standards for the differing disciplines within Information and Records Management. 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 shown in the diagram below:



Characteristics of an Authoritative Record

Record	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

Document Classification
All information possesses a security classification. The Cabinet Office Government Security Classifications 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 Sensitive' under the 2014 scheme.

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 health record. Other records will need to fulfil criteria as being worth keeping, such as business documents or emails**.**

Managing Electronic Records
Digital information must be stored in such a way that it can be recovered in an accessible format, in addition it must provide details of those people 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 to 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 should be remembered that any links that are used must be kept up-to-date as the record 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.

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.

Information Governance
Please refer to the Trust's suite of formal Information Governance documents for further details on the security and governance of personal information. This is available on the network share (drive) G:\DocumentLibrary\UHPT Trust Documents\Information Governance.

Individual Policy Standards
Managing Health Records Standard Operating Procedure – See Appendix 1.

7 Consultation and Ratification

The design and review process of this policy document will comply with The Development and Management of Trust Wide Documents. G:\DocumentLibrary\UHPT Trust Documents\Corporate Records Management\The Development and Management of Formal Documents.pdf

The review period for this document is set at three years since the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the policy described.

This document will be approved and reviewed by the HRSG and ratified by the Director of IM&T (CIO).

Non-significant amendments to this document may be made with delegated authority from the Head of Health Records. These must be reported retrospectively and ratified by next available meeting of the HRSG.

Significant reviews and revisions to this document will include a consultation with all sub-groups of the CIGAC and the HRSG. For non-significant amendments consultation will be restricted to the HRSG.

8 Dissemination and Implementation

Following approval and ratification this policy will be:

- Rolled out across the Trust
- Publicised in Vital Signs the Trusts weekly staff news briefing
- Made available on the network share (drive) G:\DocumentLibrary\UHPT Trust Documents

- The Policy will be highlighted in any Records Management and Information Governance Training and Trust wide Induction and Mandatory training

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 and record management, and that they are competent in carrying out their designated duties.

Case Note Training is a mandatory course that is completed every two years for all Administrative and Clerical staff and Nurses/HCA's who deal with case notes within their line of work. The Health Records Support Team enrols all staff onto the training which includes new starters to the Trust, existing staff members who are due to complete their training, requested by staff member, requested by Line Manager or a need to complete the training has been identified following examples of poor working practice.

Audits are completed on all staff members who complete the Case Note Training Programme. The Health Records Support Team reviews five sets of Case Notes per audit. Results of the audits are communicated to the staff member and their Line Manager. The pass rate for an audit is set at 95%. If a staff member fails an audit then they are advised as appropriately and a repeat audit is completed within four to six weeks. The Health Records Support Team will complete a Datix incident form if there are significant concerns about working practices identified.

Audits are also completed on all Wards and Departments in the Trust by the Health Records Support Team on a six monthly basis. The results of these audits are communicated to the Ward Clerk and their Line Manager. The HRCO will escalate to the CRL Manager (Governance) any staff member, ward or department that fails to engage in the Case Note Training Programme or when there are significant concerns about working practices following an audit or complaint.

9 Monitoring compliance and effectiveness

The Trust may be asked for evidence that they operate a satisfactory records management regime. There are a range of sanctions that can be applied where records management is found to fall short of the required standards. These could be formal warnings, dismissal, professional deregulation, Care Quality Commission (CQC) intervention and monetary fines. Regulatory action from the Information Commissioner's Office.

Compliance with this policy is monitored through reporting to the HRSG as follows:

- Bi-annual review regarding the progress of the Case Note Training Programme and audits by the Health Records Compliance Officer (HRCO)
- Bi-annual review of the processes involved in the retention, disposal and destruction of health records by the CRL Manager (Operations)
- Bi-annual review of the physical condition of the health records and filing of loose sheets by the HRCO
- Bi-annual audit of record availability within the Trust for planned, emergency appointments and admissions by the HRCO
- Annual review of the number of misfiles within the Central Records Library by the CRL Manager (Governance).
- Bi-annual review of random tracings on iPM (approximately 50 sets of notes are checked) by the HRCO

- Bi-annual review to check compliance within the Trust with regards to the Moving and Tracking of case notes APN by the HRCO
- Bi-annual review to check compliance with the 30 day target for the completion of Subject Access Requests (this is also reported to CIGAC twice a year) by the CRL Manager (Governance)
- Bi-annual review of all risks relating to Health Records by the CRL Manager (Governance)
- Annual review of the process for reporting incidents and complaints by the CRL Manager
- Bi-annual review of the Trust's compliance with the Change of Identity in Adopted Patients Policy and the Transgender APN on an annual basis by the HRCO
- Bi-annual review of Paper Forms and eForms by the Trusts by the eForms & Records Strategy Lead
- Bi-annual review of Double registrations and mixed patient records by the Clinical Systems Manager

The HRSG will commission ad hoc Audits, via the Health Records Support Team and/or the Clinical Audit Office when issues relating to paper record keeping are brought to their attention.
Ongoing review and implementation of recommendations and actions will be overseen by the respective steering group. This will be managed in accordance with the severity and priority of the issues and reported to CIGAC as necessary.

Detailed monitoring compliance and effectiveness for each standard area will be found at the corresponding appendices:

- **Managing Health Records Standard Operating Procedure – Appendix 1**

NB: The Quality of Clinical Record Keeping *is monitored by the Clinical Audit Department who will conduct an annual audit and report to the HRSG. (Please see the* **Clinical Record Keeping Policy** *for more detail* G:\DocumentLibrary\UHPT Trust Documents\Clinical Records Management\Clinical Records Keeping Policy.pdf

10 References and associated documentation

The Records Management Code of Practice for Health and Social Care 2016. NHS Digital. Available at:
www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

The Data Protection Act 2018.
www.legislation.gov.uk

The Access to Health Records Act 1990.
www.legislation.gov.uk

Connecting for Health (England). *Website resources*. Available at: www.connectingforhealth.nhs.uk

Department of Health. (1999). *For The Record – Managing Records In NHS Trusts And Health Authorities*. London: Department of Health. Available at: www.dh.gov.uk

Internal Documents/Policies:

- Clinical Record keeping Policy
- Information Governance Formal Documents
- System Level Security Policies
- Audio and Visual Recording Policy

See below for Health Records related APNs available at: \\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs

Trust Document - Sub Folders	TITLE	REVIEW DATE
Clinical Records – Case notes	Filing within Case note Folder (Patient Document)	Jun-22
Clinical Records – Case notes	Restricted Access and Site Security (Central Records Library, Bush Park)	Jun-21
Clinical Records – Case notes	Splitting Oversized Case note Folders	Jun-22
Clinical Records – Case notes	How to request notes from the Central Records Library	Jan-21
Outpatients Management	Prepping Case notes to Late Additions to Clinics	Jan-21
Clinical Records – Case notes	Release of Patient Case notes	Jan-21
Clinical Records – Case notes	Moving and Tracking Patient Case notes (Patient Documents)	Jun-22
Clinical Records – Case notes	Retention and Destruction of Case notes	Jan-21
Clinical Records - iPM	Recording and Filing of Living Wills and Advance Directives	Jan-21
Clinical Records – Case notes	Managing Temporary Case notes	Jun-22
Clinical Records – Case notes	Raising a New Case note Folder	Jun-22
Clinical Records – Case notes	Management of Contaminated Health Records	Apr-22
Clinical Records – Case notes	Misfiled Paperwork within another Patients Health Records	Jul-21
Clinical Records – Case notes	Missing or Lost Health Records	Feb-21

1 Standards and Practice

Health Records Creation and Identification
A new patient record (paper case note and an electronic iPM record) is created by the receiving department when a new patient is referred to the hospital and has not already been registered on iPM with a current set of notes. This may be when the patient attends the hospital for an Inpatient/Day-case or an Outpatient Appointment.

Each patient registered on iPM is allocated a unique NHS Number and a local identification number (the Hospital Number). All NHS electronic systems use the NHS number as well as other identifiers.

Emergency admissions, not registered, will have case notes created either by the Emergency Department (if being admitted to the hospital) or by the admitting Ward. If the patient cannot be identified then staff should refer to the **'Raising a New Case Note Folder APN** available on the network share (drive) G:\DocumentLibrary\UHPT Trust Documents/APNs

New Electronic Health Records will be created on other Trust electronic systems, aside from iPM, as required to support the patient care.

It is essential that new episodes of care for existing Patients are always added to the existing Patient Record. Creating a new record will lead to duplication and compromise the integrity of the Patient's record.

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

Electronic patient record systems should feed directly from the Hospitals Patient Administration System, as the Primary System, to ensure that the most up-to-date patient demographic information is being referenced.

Adopted Persons Health Records
Current National Guidance states that patients who have had their identity changed due to being adopted can be issued with a new NHS Number and this needs to exclude reference to their previous identity. These records can only be placed under a new surname when an adoption order has been granted. An alias may be used prior to the adoption order being granted. For detailed process please see - **Change of Identity Policy for Adopted Patients** available on the network share (drive) G:\DocumentLibrary\UHPT Trust Documents

Ambulance Records
These records will contain evidence of clinical intervention and it is necessary to treat them as a health 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 health 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 NHS England: http://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf

Family Records
These types of records are commonly seen within health visiting, some therapy services and Clinical Genetics where a holistic picture of the family is needed to deliver care. Records attributed to individuals and managed as such can create an issue for the NHS and Social Care. It may be necessary to specify one person as the focus of the record, hold the entire record and then link the other family members records together. It is imperative that any disclosure of an individual's record is scrutinised to ensure no third party information is disclosed without consent.

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 are:

- 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.

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 given to patients to hold then 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 returned to the issuing organisation. An example of this is a hand held 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: http://sytems.hscic.gov.uk/infogov/codes.cop

Records of Funding
These are primarily administrative records but do contain large amounts of care information and therefore must be managed as health 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 to ensure their wishes relating to the management of their records and information. 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 (GRA) 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. \\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs\Equality and Diversity\Gender Reassignment Cases.pdf

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.

Dental study models
The Oral and Maxillofacial Surgery and Dental Specialities Department in the Trust retain dental study models (these are plaster models of patient's teeth and their relationship).

The above Departments are responsible for the storage, retention and destruction of these models. The department follows the guidance from The British Orthodontic Society (2015) for England & Wales and the guidance from the Records Management Code of Practice for Health and Social Care 2016.

Study models will be retained as follows;

CHILD: until the patient's 25th birthday or 26th if an entry was made when the young person was 17 at the conclusion of treatment, or 8 years after death.

ADULT: 10 years after conclusion of treatment, the patient's death or after the patient has permanently left the country.

CANCER: Retain any models for patients who have (or had) head and neck cancer for 30 years or 8 years after the patient has died.

IMAGES: Photographs, xrays films (including digital) and radiographic reports to be treated as a part of the patients health record.

AUDIT: records 5 years.

Record Keeping
Please see Trusts **Clinical Record Keeping Policy** for further information and help. G:\DocumentLibrary\UHPT Trust Documents\Clinical Records Management\Clinical Records Keeping Policy.pdf

Using health records for virtual activity (telephone and video consultations)
The Trust recognises that in some circumstances Clinicians will be undertaking consultations via the use of telephone or video solutions and this activity could be completed within the Trust or from their own home. This could be due to lack of outpatient capacity within the Trust, due to a further outbreak of COVID-19 in the region or another epidemic/pandemic scenario. To support this process and to adhere to this policy and the Trust's Clinical Record Keeping Policy the Clinician and Service Line Management Team will need to do the following:

1. Clinician to agree formally with the Service Line their intention for working remotely using a virtual solution.
2. Service Line to liaise with the Information Governance Team and Health Records Management Team regarding the change in process to identify any risks to patient information and the health records.
3. Service Line to liaise with the IT department to ensure the Clinician has the necessary equipment to complete the work remotely.
4. Service Line to arrange the requesting of the health records needed for the activity. A risk assessment will need to be completed if the health records are required to leave Trust premises and be used in the Clinician's home for example. Please see Transporting/Transmitting Health Records section on page 29 and the Staff Transporting Case Notes off site section on page 30 for more information.
5. Clinician must write a summary of the activity on a clinical record sheet which is held within the patient's health record thus ensuring the record is up to date. A typed clinic letter will also be filed within the health record once produced after the appointment.
6. Clinician to return the health records to the Trust in a timely fashion so they are available for use as needed by other Trust staff.
7. Service Line must ensure all health records that leave the Trust are tracked on iPM with a telephone number added to the comments section so the records can be requested should they be needed urgently. (In cases where a large number of health records are leaving the Trust the Service Line will be asked to maintain a spreadsheet detailing the patient's health records used, when the records left the

Trust and when they were returned. This document will need to be shared with the Health Records Management Team).

8. If an incident occurs due to patient's health records being used at a Clinician's home then this needs to be reported as normal through the Datix system with the Health Records Management Team being informed.

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 Support Team can change a temporary case note to the main case note after thorough investigation when the previous case note has been missing for a year or more.

There may be occasion when two records on the Patient Administration System appear to be for the same patient. In this instance the Clinical Systems Team must be contacted. The Clinical Systems Team (Merge) 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.

Storage of Paper Health Records

Health Records Libraries

Health Records Libraries must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health & Safety at Work Act 1974 and Workplace (Health, Safety and Welfare) Regulations 1992.

Central Records Library, Bush Park

The Central Records Library (CRL) is the Trust's primary off-site store for Health Records. CRL staff will ensure that records stored within the CRL are traced and filed appropriately, are available when needed and dispatched in a timely manner when needed, to avoid undue delay to patient care.

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. Firefighting equipment and alarms must comply with current standards and be inspected regularly. There should be appropriately sited smoke alarms that are inspected regularly.

Equipment
There are adequate safety stepladders and safety tools.

Filing
Health records will be filed in Terminal Digit Format.

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

Requests for Health Records filed in the Central Records Library
The Health Records Library at Bush Park is open Monday to Friday between 08:00 and 20:00 and between 09:00 and 16:30 on Saturday and Sunday. All Bank Holidays are covered by staff working between 09.00 and 17.00.

The urgent line (ext 30421) is manned Monday – Friday 08:00 – 20:00
Saturday & Sunday 09:00 – 16:30 and Bank Holidays – 09:00 – 17:00
Urgent Room Collections are made every hour on the half hour. The notes are then delivered to Derriford Hospital by Saba within half hour to an hour of collection from Bush Park.
Weekend and Bank Holidays – Urgent notes are delivered directly to the requestor and not the Urgent Room. When taking urgent requests please note the specific location for the Saba Team and whether rooms/doors have codes to enter and have been specified by the requestor.

Requests for health records outside of these hours should be through the MAU Ward Clerks, Level 6 of the Hospital. They can be contacted via extension 39478, 01752 439478 or bleep number 0954. Requests to MAU to retrieve notes out of hours must only be made for clinically urgent cases and non-urgent requests should be sent to Bush Park the following day. Records are retrieved out of normal office hours by the MAU Ward Clerks accompanied by a member of the Security Team. It is Security's responsibility to deactivate and activate the security alarm at Bush Park. MAU Ward Clerks will trace the Health Records upon returning to the hospital.

Off Site Storage

The Trust has a contract with an external company (Crown Records Management) providing secure storage for its archived deceased and non-current health records. Off-site storage must conform to all the same relevant legislation as if they were filed on site at UHP. Non-current health records are those that have not been seen between three and eight years and deceased patients. Childrens and maternity records, which are kept for 25 years might also be archived off site. UHP retains the records maintenance function of these records; this does not lie with the external contractor.

Storage of case notes in other areas

Offices

Offices must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health & 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 outside of the CRL 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 Security/Porters so that they are accessible out of normal office hours. All health records must be electronically tracked to the office location.

All staff that handle records must ensure that records held within their department are:

- Secure (i.e. never left unattended in public places and accessible on a strictly need to know basis)
- Traced in on receipt and out on dispatch on the iPM system
- Are available when needed and dispatched in a timely manner to avoid undue delay to patient care

Wards and Hospital Departments

Whilst 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 faced down so that the information cannot be read by unauthorised people.

Availability of records

Health records should be available for every patient each time they attend hospital. All health records must be obtained as soon as possible following admission to a Ward by the Ward Clerk. Ward Clerks must check daily that all health records are available or have been requested and have an expected time frame for their arrival from Bush Park or other location.

All health records must be electronically tracked each time they are moved between locations, failure to do so may result in missing records.

Health records in use outside of the main Library are the responsibility of the individual recorded on the tracking on iPM.

Missing/Lost records
A thorough search must be made of all locations within the area where the health records have been tracked. Check with your colleagues as to whether they have seen the health records. Use the Trusts communication systems, email, telephone etc….to enquire from other wards/departments if the health records are in their area. Use Hospital Number (HN's) and initials only when using the email 'Noticeboard'.
If health records cannot be located then contact the Central Records Library via extension 37213 / 38084 or crl.helpdesk@nhs.net. Searches can be completed at Bush Park for the health records. If the health records have been misfiled at Bush Park then routine checks will be made. Please see the Trusts APN Missing or Lost Health Records. \\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs
A Datix incident form should be completed in the event of a missing Health Record.

Transporting/Transmitting Health Records

Between The CRL and Derriford Hospital
All health records in transit must be in either a blue box, blue or orange bag or brown sealed envelopes, and either moved by Saba, the Trust's approved Courier Service or the contracted Taxi company. Vehicles used for transporting health records between hospitals should be:

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

All boxes, bags and envelopes must be clearly labelled with the destination, 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 containing personal identifiable information being transported between departments and wards must either be in blue bags or in an envelope which is securely fastened. All bags and envelopes must be clearly labelled with the destination, to ensure that health records do not go missing or end up in the wrong place.

Patients transporting own case notes between different sites
It is not appropriate for patients to transport their own case notes between different sites. This restriction is in place to control the risk of case notes becoming lost, mishandled and to reduce the potential distress the patient could experience from reading the content of their notes unsupervised. This means patients cannot take their case notes home or from Derriford Hospital to another site including Rowan House, Nuffield Hospital, Mount Gould Hospital and the Dialysis Unit etc.

Patients carrying own case notes within the same building
If a patient has appointments within the **same** building on the **same** day then patients can carry their own case notes with them, but the case notes MUST be placed in a brown sealed envelope. Staff are required to be vigilant whilst going about their daily duties and are required to address any issues if they see any patients accessing and/or reading their case notes unsupervised. If this does occur then this incident must be reported via Datix.

If staff suspect case notes have been tampered with or viewed by a patient they should notify the Health Records Support Team via plh-tr.casenotemgtqueries@nhs.net. Please see the Trusts APN Moving and Tracking Patient Case Notes. \\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs

Staff Transporting Case notes off site (including their home)
Where patient identifiable information or patient case notes are taken off site, the following guidance must be observed.

Staff should not leave portable computers, medical notes or mobile data devices (e.g. Dictaphones, PDAs, digital cameras) that are used to store patient case notes/patient identifiable information in unattended cars or in easily accessible areas. Ideally staff should store all files and portable equipment under lock and key, when not actually being used.

If staff need to take case notes to other hospitals, patients home or their home for any reason then procedures should be in place to safeguard that information effectively.

This includes the following actions:

- Undertaking a risk assessment ensuring the storage and safety of the case notes at all times that they are away from UHPT
- Putting in place systems to ensure the case notes can be accessed in an emergency if needed
- Ensuring that the case notes are traced out and the current location is traceable and accessible. Adding a contact telephone number to the comments section on iPM should the notes be needed urgently
- Ensuring that permission has been given by their Line Manager for the case notes to be transported off site by the individual

Any case notes taken off site must be properly secured preferably within a container in the boot of the car or the rear of the van; they should never be on open view on a seat. Staff transporting Health Records should never leave their vehicles unlocked.

Release of Patient Case Notes
If a patient or relative requests access to their case note, or other hospitals and other authorities such as Police and Solicitors please see the Trusts APN Release of Patient Case Notes. \\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs

If a patient is having a planned outpatient appointment or inpatient admission at another hospital (UHP Trust activity) then the patients' case notes can be tracked and sent to this location.

If a patient is being transferred from Derriford Hospital to another hospital for continuing treatment then please see the flowchart (Appendix 1) in the APN Moving and Tracking Patient Case Notes. \\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs

Red 'Unidentified Patient' case note folders (known as QQ folders) are not to be released from Derriford Hospital, except to the Merge Team for amalgamation. Please see the Trusts Unidentified and Hospital Trauma Patients Standard Operating Procedure. \\derriford\groups\DocumentLibrary\UHPT Trust Documents

Records or copies of records sent to other Hospitals

Where copies of Health records are requested by other hospitals for treatment purposes please contact the Disclosure Team via plh-tr.DisclosureTeam@nhs.net. If copies are requested by other hospitals for research purposes or relating to a clinical trial then please contact the Research and Development Team. Copies of records must be legible and reflect the original record. Please see the Trusts APN Release of Patient Case Notes and Subject Access Request Policy.
\\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs.
\\derriford\groups\DocumentLibrary\UHPT Trust Documents\Clinical Records Management\Subject Access Request (SAR) Policy.pdf

Right of rectification requests
Under Data Protection Legislation; UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR) 2018, data subjects have certain rights, one of these is the "right of rectification".

If a Data Subject considers any information contained within their records to be inaccurate, they can request the information be corrected/completed.

It should be noted, however, that diagnosis and clinical opinion is a matter of clinical judgement and cannot be changed solely at the patient's request.

A Right of Rectification Standard Operating Procedure has been produced which the Disclosure Team and the Health Records Management Team will follow this for requests received in the Trust. The HR Department will handle any requests to rectify information held within a personnel/employee record and will follow their own process with this document being used as guidance.

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 healthcare 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.

Patient information can be emailed as an interim solution until such time as clinical messaging is embedded into our clinical systems.

The Trust uses NHSmail as its primary email service which is secure for the transmission of person identifiable information relating to patients or staff between other NHSmail users.

Information should be restricted to the minimum that is necessary and strictly only sent to those staff that have a specific need to know.

Personal data should not be circulated to large distribution lists unless each staff member has a definite need to know. For example, emails regarding missing case notes sent to the PHNT Noticeboard should be restricted to initials and hospital number only.

If sending person identifiable data by email from NHSmail to a non NHSmail email address then NHSmail encryption **must** be used.

Please reference the Policy which can be located in the Trust's Document Library. \\derriford\groups\DocumentLibrary\UHPT Trust Documents\Information Governance\Disclosure of Personal Information by Email SOP.pdf

Faxing Information
The Trust no longer supports the general use of fax machines. Fax machines can be used in an emergency situation when other methods of transmitting information are not available, the fax machine must be located in a Safe Haven.

For the use of mobile devices to transport/transmit Information - Please see the Trusts **Audio and Visual Recording Policy** located in the Trust's Document Library. \\derriford\groups\DocumentLibrary\UHPT Trust Documents\Information Governance\Audio and Visual Recording Policy.pdf

Management of Patient Records
Procedures relating to iPM and case notes, are governed by Administrative Procedure Notes (APN's) which are located in the Trust's Document Library \\derriford\groups\DocumentLibrary\UHPT Trust Documents\APNs

Other electronic Patient Record Systems are managed by the respective Systems Managers who detail the governance in their respective System Level Security Policy (SLSP).

Retention, Disposal and Destruction of Case notes
There are three principal options regarding how to process a record that has exceeded its minimum retention period:

Destroy
When a record meets its minimum retention time it would usually be destroyed in accordance with agreed Trust procedures (see APN) unless the HRSG has agreed that the records should be retained for a further period.

Dispose (i.e. by passing on to another organisation)
This only applies to records belonging to Service Personnel. These are retained until the appropriate retention period expires and are then sent securely to MOD Shoeburyness to be processed.

Retain for a further period
Where a record type is not listed or a health professional requires that specific records be retained beyond the minimum retention period, then this should be brought to the attention of the Trust's CRL Manager (Governance).

The HRSG make the final decision on such matters in order to balance the interests of professional staff, the resources available for storage and to give consideration to the fifth principle of the Data Protection Act, that 'Personal data … shall not be kept for longer than is necessary for that purpose or those purposes'. Such decisions will be clearly documented in the minutes of the HRSG meeting.

The Trust has a Records Maintenance and Archive Service based within the Central Records Library. Members of this team have been specially trained to process Health Records according to agreed national and local requirements and are therefore the **only** members of Trust staff authorised to undertake the archiving, destruction and/or disposal of Health Records.

The Records Maintenance and Archive Service ensure that a permanent record of the destruction and disposal of patient case notes is entered onto iPM and that *secure destruction certificates* are obtained whenever notes are taken away to be destroyed.

Retention, Disposal and Destruction arrangements for records held on electronic systems are detailed in the respective System Level Security Policies (SLSP).

The Independent Inquiry into Child Sexual Abuse

The Inquiry has issued retention instructions to a range of institutions requesting the preservation of all records relating to the care of children so that they remain available for inspection by the Inquiry.

Justice Goddard also stated in her opening statement on 9 July 2015 that "No institution – whether they have received a letter or not – can be in any doubt of the extent of their duty to preserve records for the Inquiry, or of the consequences of failing to do so" (paragraph 77).

The Inquiry received a number of queries about the possibility that prolonged retention of personal data in accordance with the retention instructions might engage issues of compliance with data protection legislation. The Inquiry consulted with the Information Commissioner's Office and, having done so, issues this Guidance to clarify the position. Under Section 21 of the Inquiries Act 2005 the Inquiry has the power to order the production of documents. Failure to comply with such an order without reasonable excuse is an offence punishable by imprisonment (Section 35 of the Inquiries Act 2005).

It is also an offence for a person, during the course of an Inquiry, to destroy, alter or tamper with evidence that may be relevant to an Inquiry, or deliberately to do an act with the intention of suppressing evidence or preventing it being disclosed to the Inquiry.

Institutions therefore have an obligation to preserve records for the Inquiry for as long as necessary to assist the Inquiry. Prolonged retention of personal data by an organisation at the request of the Inquiry would not therefore contravene data protection legislation, provided such information is restricted to that necessary to fulfil any potential legal duties that organisation may have in relation to the Inquiry.

An institution may have to account for its previous activities to the Inquiry so retention of the data will be regarded as necessary for this purpose. The obligation to the Inquiry to retain documents will remain throughout its duration. Institutions may also incur separate legal obligations to retain documents during the course of the Inquiry, for example in relation to other legal proceedings.[3]

Once the Inquiry (IICSA) has completed its investigation and has released the Trust from the obligations referred to above, the Trust will revert to adherence to the minimum retention periods set out in the *Records Management Code of Practice for Health and Social Care, 2016* unless there are separate inquiries ongoing – see below regarding the Infected Blood Inquiry.

Infected Blood Inquiry

[3] Guidance Note: Retention Instructions and Data Protection requirements (version 2) 25th July 2018

This is an independent public statutory Inquiry established to examine the circumstances in which men, women and children treated by national Health Services in the United Kingdom were given infected blood and infected blood products, in particular since 1970.

In July 2018 NHS England received communication from the Chair of the Inquiry giving notice of retention/non-destruction of documents relating to the Inquiry. Therefore all health records are being retained.

Please refer all requests for information contained within health records quoting this inquiry or IICSA to the Trusts Disclosure Team.

Risk Management, Disaster Planning and Business Continuity

Regular risk assessments are undertaken in line with the Trust's Risk Management Strategy. Risks are recorded locally or on the Trust's Datix Risk Management module and reviewed in a timely manner. All incidents reported relating to health records through the Trusts Datix Incident Reporting module will be reviewed and responded to in a timely manner, and discussed and monitored at the HRSG as appropriate.

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. The CRL has a Business Continuity Plan which is 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.

Health Records Training

All administrative and clerical staff and Nurses/HCA's who deal with case notes within their line of work are required to complete mandatory case note training every two years.

Information Governance training is mandatory and is incorporated in Trust Induction and Mandatory Training.

All staff who use iPM in the course of their work are required to attend the relevant modular systems training before access is given to the system. Comprehensive manuals and eLearning are available for each iPM module and can be found on ESR - Employee Self-Service (https://my.esr.nhs.uk).

Training to use other electronic systems will be provided by the relevant System Managers.

Core Information	
Document Title	Health Records Policy
Date Finalised	August 2020
Dissemination Lead	Head of Health Records
Previous Documents	
Previous document in use?	Electronic versions only
Action to retrieve old copies.	Old version superseded on Trust Documents Network Share

Dissemination Plan

Recipient(s)	When	How	Responsibility	Progress update
All Staff	Within 4-weeks of ratification	Vital Signs	Head of Health Records	
All Staff	Within 4-weeks of ratification	Trust Documents on Staffnet	Head of Health Records	
All Staff	Within 4-weeks of ratification	Trust induction and mandatory training	Head of Health Records	

Review and Approval Checklist	Appendix 3

Review		
Title	Is the title clear and unambiguous?	Yes
	Is it clear whether the document is a policy, procedure, protocol, framework, APN or SOP?	Yes
	Does the style & format comply?	Yes
Rationale	Are reasons for development of the document stated?	Yes
Development Process	Is the method described in brief?	Yes
	Are people involved in the development identified?	Yes
	Has a reasonable attempt has been made to ensure relevant expertise has been used?	Yes
	Is there evidence of consultation with stakeholders and users?	Yes
Content	Is the objective of the document clear?	Yes
	Is the target population clear and unambiguous?	Yes
	Are the intended outcomes described?	Yes
	Are the statements clear and unambiguous?	Yes
Evidence Base	Is the type of evidence to support the document identified explicitly?	Yes
	Are key references cited and in full?	Yes
	Are supporting documents referenced?	Yes
Approval	Does the document identify which committee/group will review it?	Yes
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	Yes
	Does the document identify which Executive Director will ratify it?	Yes
Dissemination & Implementation	Is there an outline/plan to identify how this will be done?	Yes
	Does the plan include the necessary training/support to ensure compliance?	Yes
Document Control	Does the document identify where it will be held?	Yes
	Have archiving arrangements for superseded documents been addressed?	Yes
Monitoring Compliance & Effectiveness	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes
	Is there a plan to review or audit compliance with the document?	Yes
Review Date	Is the review date identified?	Yes
	Is the frequency of review identified? If so is it acceptable?	Yes
Overall Responsibility	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes

Equalities and Human Rights Impact Assessment	Appendix 4
Core Information	
Manager	Vanessa Bennett
Directorate	IM&T
Date	August 2020
Title	Health Records Policy
What are the aims, objectives & projected outcomes?	To support the provision of high quality care by ensuring Health Record and Information Management complies with the relevant legislation and regulatory requirements and that health records are: • Secure • Retained and disposed of appropriately • Available when needed • Can be interpreted • Can be trusted • Can be maintained through time • And that staff are trained in health records management in accordance with the policy
Scope of the assessment	
This policy has limited equalities and human rights impact, all staff have been consulted and this policy is available in all forms of communication upon request and contains no restriction or prejudice to any group	
Collecting data	
Race	N/A
Religion	N/A
Disability	N/A
Sex	N/A
Gender Identity	N/A
Sexual Orientation	N/A
Age	N/A
Socio-Economic	N/A
Human Rights	N/A
What are the overall trends/patterns in the above data?	N/A

Specific issues and data gaps that may need to be addressed through consultation or further research	N/A
Involving and consulting stakeholders	
Internal involvement and consultation	N/A
External involvement and consultation	N/A
Impact Assessment	
Overall assessment and analysis of the evidence	N/A

Action Plan				
Action	**Owner**	**Risks**	**Completion Date**	**Progress update**