Pennine Care
NHS Foundation Trust

DOCUMENT CONTROL	
Title:	**Records Retention Policy**
Version:	**4**
Reference Number:	**RM006**

Scope:

This guidance applies to all health, business and corporate records held in *any* format by the Trust. The Trust's records management duty includes responsibility for the records legacy of predecessor organisations and any obsolete services.

Due to the Independent Inquiry into Child Sexual Abuse all records should be retained until further notice. This means all clinical and corporate records in whichever format held i.e. paper or electronic.

For further information please contact the Records Manager

Purpose:

The purpose of this document is to provide guidance to the retention of records in line with the Records Management Code of Practice for Health and Social Care 2016.

Requirement for Policy

To comply with the General Data Protection Regulation, Data Protection Act 2018, Data Protection and Security Tool and the Records Management Code of Practice for Health and Social Care 2016.

Keywords:

Health records, mental health, community, staff files, records, management, retention, appraisal, Caldicott Guardian, Code of Practice

Supersedes:

Version 3

Description of Amendment(s):

Was previously known as CO098
Updated in line with the GDPR
Health Records of Transgender Patients

Owner:

Records Manager – Carole Trodden

Accountability:	
• Trust Solicitor • Director of Service Development and Delivery	
Individual(s) & group(s) involved in the Development:	
This document has been developed in collaboration with the following interested parties: • Carole Trodden • Kuldip Sohanpal	
Individual(s) & group(s) involved in the Consultation:	
The document has been circulated for consultation and comments have been taken into consideration and the document amended accordingly: • Members of IGMM • Members of IGAG	
Equality Impact Analysis:	
Date approved:	4th February 2019
Reference:	RM006-EIA006
Freedom of Information Exemption Assessment:	
Date approved:	8th February 2019
Reference:	POL2018-96
Information Governance Assessment:	
Date approved:	8th February 2019
Reference:	POL2018-96
Policy Panel:	
Date Presented to Panel:	11th February 2019
Presented by:	Carole Trodden
Date Approved by Panel:	11th February 2019
Policy Management Team tasks:	
Date uploaded to Trust's intranet:	12th February 2019
Date uploaded to Trust's internet site:	12th February 2019

Review:	
Next review date: **Responsibility of:**	February 2022 Records Manager
Other Trust documentation to which this policy relates (and when appropriate should be read in conjunction with):	
RM001	Records Management Policy
RM002	Moving/Transferring of Bulk Paper Records Procedure
RM003	Management of Mental Health & Specialist Services Health Records Guidance
RM007	Management of Community Services Health Records Guidance
RM005	Management of Business and Corporate Records Management Guidance
RM004	Missing Records Procedure
Policy Associated Documents:	
TAD_RM006_01	Records at Contract Change
TAD_RM006_02	Records Retention
Other external documentation/resources to which this policy relates:	
	Records Management Code of Practice for Health and Social Care 2016 https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016
	General Data Protection Regulation 2018 https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation
	Data Protection Act 2018 https://www.gov.uk/government/collections/data-protection-act-2018
	Caldicott Principles 2013 https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx
	Ministry of Justice: Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (2009): https://ico.org.uk/media/for-organisations/research-and-reports/1432475/foi-section-46-code-of-practice-1.pdf
	The National Archives: http://www.nationalarchives.gov.uk/

	Professional Record Standards Body for health and social care: http://theprsb.org/standards-matters/
	Information Governance Alliance: www.hscic.gov.uk/iga
	Information Commissioner's Office: https://ico.org.uk/
	Department of Health Information Governance Toolkit (hosted by the HSCIC): https://nww.igt.hscic.gov.uk/
	https://www.cqc.org.uk/sites/default/files/documents/guidance_about_compliance_summary.pdf
CQC Regulations **This guideline supports the following CQC regulations:**	
Regulation 17	Good Governance

Contents Page

1.	Introduction	7
2.	Purpose	7
3.	Responsibilities, Accountabilities & Duties	8
4.	Place of Deposit (PoD)	9
5.	Appraisal of Records	11
6.	Destruction/Erasure of Paper and Electronic Records	11
7.	Records at Contract Change	12
8	How to deal with specific types of records	13
8.1	Prison Health Records	13
8.2	Youth Offending Service Records	13
8.3	Secure Units for Patients detained under the Mental Health Act 1983	13
8.4	Family Records	14
8.5	Child School Health Records	14
8.6	Integrated Records	14
8.7	Integrated Viewing Technology and Record Keeping	14
8.8	Complaints Records	15
8.9	Specimens and Samples	15
8.10	Continuing Care Decisions Records	15
8.11	Records of Funding	16
8.12	Adopted Persons Health Records	16
8.13	Health Records of Transgender Persons	16
8.14	Witness Protection Health Records	17
8.15	Controlled Drugs Regime	17

8.16 Asylum Seeker Records 17

8.17 Occupational Health Records 17

8.18 Records of Non-NHS Funded Patients treated on NHS premises 17

8.19 Patient/ Client Held Records 17

8.20 Records dealt with under the NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000 18

9. Equality Impact Analysis 18

10. Freedom of Information Exemption Assessment 18

11. Information Governance Assessment 19

12. Safeguarding 19

13. Monitoring 19

14. Review 19

FOREWORD

At the time of updating this guidance the Independent Inquiry into Child Sexual Abuse (IICSA) has requested that NHS and Social Care bodies do not destroy any records that are, or may fall, into the remit of the Inquiry. This includes children's records and any instances of allegations or investigations or any records of institution where abuse has, or may have occurred. Additional guidance will be published if this should change.

1. INTRODUCTION

This guidance sets out the minimum periods for which the various records created within the Trust should be retained, either due to their on-going administrative value or as a result of statutory requirement. It also provides guidance on dealing with records, which have on-going research or historical value and should be selected for permanent preservation as archives and transferred to a Place of Deposit approved by The National Archives.

This guidance provides information and advice about all records commonly found within NHS organisations and includes both clinical and corporate records. Clinical records are those records used in the treatment/care of patients or service users whereas corporate records relate to the business administrative function such as finance, HR, Estates etc.

The retention schedule applies to all the records concerned, irrespective of the format (e.g. paper, electronic, databases, e-mails, X-rays, photographs, CD-ROMs) in which they are created or held.

2. PURPOSE

Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. **The retention periods listed in this schedule must always be considered a minimum.**

Article 5 (e) of the GDPR states personal data shall be kept for no longer than is necessary for the purposes for which it is being processed. There are some circumstances where personal data may be stored for longer periods (e.g. archiving purposes in the public interest, scientific or historical research purposes).

Recital 39 of the GDPR states that the period for which the personal data is stored should be limited to a strict minimum and that time limits should be established by the data controller for deletion of the records (referred to as erasure in the GDPR) or for a periodic review.

Records should always be reviewed at the point that records reach their retention period as the Trust may decide to keep records longer than the recommended

minimum period, it can vary the period accordingly and the decision will be recorded and the reasons behind it within the retention schedule.

3. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

- The **Chief Executive** has overall responsibility for ensuring that records are managed responsibly within the Trust. As Accountable Officer, the Chief Executive is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this, as it will ensure appropriate, accurate information is available as required.

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

- The **Executive Director of Service Development and Sustainability is the Senior Information Risk Officer (SIRO)** for the Trust. The SIRO has overall responsibility for the organisation's information risk policy and will also lead and implement the information governance risk assessment and advise the Board on the effectiveness of risk management across the organisation.

- The Trust's **Caldicott Guardian** acts as the 'conscience' of the Trust in relation to person identifiable information and actively supports work to facilitate and enable information sharing. The Medical Director is the Caldicott Guardian and is responsible for ensuring person identifiable information is shared in an appropriate and secure manner. The Caldicott Guardian is the nominated Executive lead for all health, business and corporate records. The Caldicott Guardian also has a fundamental role around ensuring that the Trust is compliant with the GPDR and that personal data shall be kept for no longer than is necessary for the purposes for which it is being processed

- The Divisional Business Units (DBU's) are responsible for implementing any action plans arising from non-compliance to the Records Management Policy.

- The **Records Manager** is responsible for the overall development and maintenance of records management practices throughout the Trust. In particular, the Records Manager is responsible for drawing up guidance for good records management practice and promoting compliance with this guidance in such a way as to ensure the easy, appropriate and timely retrieval of service user information and retention periods are adhered to.

- The responsibility of local records management is devolved to the service directors and department managers. **Information Asset Owners** (IAO's) such as, Service Directors, Heads of Departments, other units and business functions within the Trust have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policy and protocols. The IAO's are supported by the **Information Asset Managers** (IAM's) who will coordinate the identification of information assets within their remit and will assign an **Information Asset Administrator** (IAA) for each asset.

- **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 in the Trust and manage those records in keeping with this retention schedule and with any guidance subsequently produced.

4. PLACE of DEPOSIT (PoD)

Retention periods given in this 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 (typically 2-5%) of key records which will:

- Enable the public to understand the working of the organisation and its impact on the population it serves and;
- Preserve information and evidence likely to have long-term research value.

Records must be selected in accordance with the guidance contained within the Records Management Code of Practice for Health & Social Care 2016 and any supplementary guidance issued by the National Archives or local guidance from the relevant PoD. Records may be selected as a class (for example Board minutes) or at lower levels such as individual files or items by the Records Manager/ Caldicott Guardian or Information Governance Manager. Any records being transferred to a PoD will be reported to the Information Governance Assurance Group. Where it is known a record will form part of the public record at creation, it must be preserved within the Trust until such time it can be transferred. The retention periods must be applied at creation and not part of a reactive process such as organisational change.

Any health records selected should normally be retained within the Trust until the patient is known, or assumed to be, deceased. This is so that they can continue to be readily available to support further medical care if necessary.

The selection of any health records for transfer to PoD should only be agreed after consultation with the appropriate clinician's, including the Caldicott Guardian and research lead.

The following factors should be taken into account when considering selection of health records:

- The organisation has an unusually long or complete run of records of a given type;
- The records relate to population or environmental factors peculiar to the locality;
- The records are likely to support research into rare or long-term conditions;
- The records relate to an event or issue of significant local or national importance (for example a public inquiry or a major incident);
- The records relate to the development of new or unusual treatments or approaches to care and/or the organisation is recognised as a national or international leader in the field of medicine concerned;
- The records throw particular light on the functioning, or failure, of the organisation, or the NHS in general;
- The records relate to a significant piece of published research.

Health records are problematic to preserve permanently in an archive or by the organisations that created them. Following appraisal, health records or a series of records, may be worthy of permanent preservation for reasons other than care, e.g. archiving purposes in the public interest, scientific or historical research purposes.

Where the patient has died, and Data Protection legislation no longer applies, the FOIA becomes the relevant legislation as the FOIA applies regardless as to whether the individual is or is not alive.

Section 41 of the FOIA and the duty of confidence remains relevant and the records cannot be accessed by anyone who does not have a lawful basis to view the records. Section 41 will therefore apply if the applicant does not have a claim under the Access to Health Records Act 1990 and the duty of confidence will need to be considered. An exemption will apply if the disclosure of the information would constitute a breach of confidence actionable by that or any other person.

When a person is deceased the Access to Health Records Act 1990 may be used to access the health record for a limited purpose by specified individuals. Therefore FOIA decisions indicate that, in general, clinical information will remain confidential for several decades after death. The duty of confidence must always be considered to apply unless there can be no persons who would suffer a detriment if the information were released. This is often quoted as 100 years but will be different for every case[1].

[1] The National Archives -
Access to NHS Records transferred to places of deposit under the Public Records Act 1958:
http://www.nationalarchives.gov.uk/documents/information-management/access-to-nhs-records-transferred-to-places-of-deposit.pdf

5. APPRAISAL OF RECORDS

The process of deciding what to do with records when their business use has ceased is called appraisal.

There will be one of three outcomes from appraisal:

- Erase/Destroy
- To keep for a longer period
- To transfer to a place of deposit.

Staff in the operational area that ordinarily uses the records will usually be able to decide whether to erase/destroy or keep for a longer period. Operational managers are responsible for making sure that all records are periodically and routinely reviewed to determine what can be erased or destroyed in the light of local and national guidance.
Once the appropriate minimum period has expired, the need to retain records further for local use should be reviewed periodically. Because of the sensitive and confidential nature of such records and the need to ensure that decisions on retention balance the interests of professional staff, including any research in which they are or may be engaged, and the resources available for storage, it is recommended that the views of the profession's local representatives should be obtained.
Electronic records can be appraised if they are arranged in an organised filing system which can differentiate the year the records were created and the subject of the record. If electronic records have been organised in an effective file plan or an electronic record keeping system, this process will be made much easier. Decisions can then be applied to an entire class of records rather than reviewing each record in turn.

6. DESTRUCTION/ ERASURE OF RECORDS

- **Paper**: paper records can be destroyed to an international standard. They can be incinerated, pulped or shredded (using a cross cut shredder) under confidential conditions. Do not use the domestic waste or put them on a rubbish tip, because they remain accessible to anyone who finds them. Confidential waste receptacles e.g. red bins/ confidential waste bags/ shredders must be used for the secure disposal of all confidential information. The relevant standard for destruction in all formats is BSIA EN15713:2009 - Secure Destruction of Confidential Material[2].
  As referenced in the retention schedule, it is important to keep accurate records of destruction and appraisal decisions. Destruction implies a permanent action. For electronic records 'deletion' may be reversed and may not meet the standard as the information can/may be able to be recovered or reversed.

- **Electronic** erasure of digital information is more challenging. Records management is concerned with accounting for information so any destruction of hard assets, like computers and hard drives and backup tapes, must be auditable

[2] BSIA EN15713:2009 - http://www.bsia.co.uk/Portals/4/Publications/form_204_id_en15713.pdf

in respect of the information they hold. An electronic records management system will retain a metadata stub which will show what has been erased**.**

- **Rights of the Individual to erasure of records –** Article 17[3] of the GDPR states that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
  1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  2. the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;[4]
  3. the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
  4. the personal data have been unlawfully processed;
  5. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
  6. the personal data have been collected in relation to the offer of information society services[5]

7. RECORDS AT CONTRACT CHANGE

Once a contract ends, any 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.

In the standard NHS contract there is an option to allow the commissioner to direct a transfer of care records to a new provider for continuity of service and this includes third parties and those working under any qualified provider contracts[6]. This will usually be to ensure the continuity of service provision upon termination of the contract. It is also the case that after the contract period has ended; the previous provider will remain liable for their work. In this instance 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 the content of records is confidential, for example health records, it may be necessary to inform the individuals concerned about the change.

[3] https://gdpr-info.eu/art-17-gdpr/
[4] https://gdpr-info.eu/art-21-gdpr/
[5] https://gdpr-info.eu/art-8-gdpr/
[6] www.england.nhs.uk/nhs-standard-contract/

Where there is little impact upon those receiving care it may be sufficient to use posters and leaflets to inform people about the change, but more significant changes may require individual communications or obtaining explicit consent. Although the conditions of the Data Protection Legislation may be satisfied in many cases there is still a duty of confidence which requires a patient or client (in some cases) to agree to the transfer.

It is vital to highlight the importance of actively managing records which are stored in off-site storage. This will ensure that the Trust maintains a full inventory of what is held off-site, retention periods are applied to each record, a disposal log is kept, and a Data Protection Impact Assessment (DPIA) is conducted on the off-site storage provider. TAD_RM006_01 summarises some possible scenarios and, for each option, patient consent and information sharing agreement or a contract may be required to share the information**.**

8. HOW TO DEAL WITH SPECIFIC TYPES OF RECORDS

8.1 PRISON HEALTH RECORDS

When the responsibility for offender health in HM Prison Service transferred from the Ministry of Justice to NHS England, a national computer based record was created to facilitate the provision of care and the transfer of care records associated with inmate transfers throughout imprisonment. However, a significant number of paper records remain and some offender health services operate hybrid paper/electronic heath records.

Prison records should be treated as hospital episodes and may be destroyed after the appropriate retention has been applied. The assumption is that a discharge note has been sent to the GP. Where a patient is sent to prison the GP record must not be destroyed but rather held until release or normal retention periods of GP records have been met.

8.2 YOUTH OFFENDING SERVICE RECORDS

Due to the nature of youth offending it is common for very short retention periods to be imposed on the general youth offending record. However for purposes of clinical liability and for continuity of care, the health care portion of the record must be retained as specified in this Code which will generally be until the 25th birthday of the individual concerned.

8.3 SECURE UNITS FOR PATIENTS DETAINED UNDER THE MENTAL HEALTH ACT 1983

Some institutions that deal with offenders are categorised as hospitals because the inmate is considered a patient. Such patient records are classed as mental health records and must be retained for longer periods of time. This is normally in excess of 30 years for purposes of the continuity of care - or another lawful basis for the continued retention is required.

8.4 FAMILY RECORDS

Family records are common within health visiting and in some therapy services where a holistic picture of the family is needed to deliver care. This creates a particular problem when the NHS and social care record keeping systems deal with the individual. It may be necessary to specify one person as the focus of the record and hold the entire record against that individual and link the other family members' records together. This will create an issue when the record is shared or disclosed in some way. Special care must be taken not to disclose information about a third party without a lawful basis to do so (for example consent).

8.5 CHILD SCHOOL HEALTH RECORDS

It is good practice for each child to have an individual record. A file for the school or a yearly intake is not considered good practice as this means the record is not about the individual child. The focus of a care record must be the individual and not the legal entity. Furthermore when a child changes school or district a record or copy must also be transferred but only when the receiving authority has confirmed that the child is resident there. Failure to carry this out properly will mean a large number of misplaced records will reside with the wrong child health or school nursing service. Where a child's record is stored on a school premises, access must be restricted to the health staff delivering care unless there is another lawful basis to access the record.

8.6 INTEGRATED RECORDS

Integrated or joint care records create additional issues which must be resolved locally. This includes a means of attributing ownership and access to the records between all parties where there is a lawful basis to access the records.
These arrangements may include:

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

For each option, some form of patient consent is necessary to enable all parties to access information lawfully which may be implied if the patient has sufficient information to inform them about the shared information and does not object. An information sharing agreement is recommended as a mechanism for providing clarity and transparency on the standards that all participants must meet and the Information Governance Department can provide guidance on this.

8.7 INTEGRATED VIEWING TECHNOLOGY AND RECORD KEEPING

Many record keeping systems pool records to create a view or portal of information which can then be used to inform decisions. This in effect creates a single digital instance of a record which is only correct at the time of viewing. Where these are used, it may be necessary to recreate the instance of viewing to allow an audit trail of decision making. It may be necessary to make a note in the record that the

information has been obtained by this means to attribute the source of evidence for any interventions taken.

8.8 COMPLAINTS RECORDS

Where a patient or client complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Complaint information should never be recorded in the clinical record. A complaint may be unfounded or involve third parties and the inclusion of that information in the clinical record will mean that the information will be preserved for the life of the record and could cause detrimental prejudice to the relationship between the patient and the health care team.

Where multiple teams are involved in the complaint handling, all the associated records must be amalgamated to form a single record. This will prevent the situation where one part of the organisation does not know what the other has done. It is common for the patient or client to ask to see a copy of their complaint file and it will be easier to deal with if all the relevant material is in one file. Where complaints are referred to the Ombudsman Service a single file will be easier to refer to. The Information Commissioner's Office (ICO) has issued guidance on complaints files and who can have access to them, which will drive what must be stored in them[7].

8.9 SPECIMENS AND SAMPLES

The retention of human material is not covered in this Code and is not in scope. The metadata or information about the sample or specimen is in scope. Relevant professional bodies such as the Human Tissue Authority or the Royal College of Pathologists have issued guidance on how long to keep human material.

Just because the human material is not kept for long periods, does not mean that the information about the specimen or sample must be destroyed at the same time. The information about any process involving human material must be kept for continuity of care and legal obligations. The correct place to keep information about the patient is the clinical record and although pathology reports may be retained by the individual pathology departments, a copy must always be included on the patient record.

8.10 CONTINUING CARE DECISIONS RECORDS

In order to process applications and appeals for funding continuing care, it is necessary for the relevant organisation to have access to clinical records. This will be based on consent and organisations need to have arrangements in place to facilitate sharing or put systems in place to allow access to view records or take copies. Any access must be lawful and the decision to grant access recorded.

[7] https://ico.org.uk/media/for-organisations/documents/1179/access_to_information_held_in_complaint_files.pdf

8.11 RECORDS OF FUNDING

Funding records are primarily administrative records but they contain large amounts of care information and as such must be managed as clinical records for their access and management. This includes having rigorous processes for access and the appropriate lawful basis to share them.

8.12 ADOPTED PERSONS HEALTH RECORDS

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

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

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

8.13 HEALTH RECORDS OF TRANSGENDER PERSONS

The Equality Act 2010 and Gender Recognition Act 2004 give trans patients legal protection against discrimination and harassment; and legal right to privacy. A transgender patient can choose which gender they wish to live their life by. It is irrelevant whether they have or are undergoing any surgery etc. to change their gender identity. They can also revert to their previous identity any time they wish. All patients (from the age of 16) are entitled under common law to be known by any name they choose, provided that there is no fraudulent intent. This includes the right to use more than one name. Patients who have chosen to ‘acquire’ a new gender can request to change their name, gender pronoun and gender details at any stage during the gender transition. They have a legal right to have their NHS care records adjusted accordingly and staff must comply with this request.

Transgender patients should consult with their GP if they wish to change their NHS number and create a new identity. The GP will carry out a process which results in the National Back Office creating a new identity with a new NHS number. The old NHS number is withdrawn so it can no longer be used. Once the Trust is informed of either the patient’s decision to change their personal details and/or the issuing of a new NHS number, all care records (paper and electronic) for that patient must be managed accurately and promptly.

8.14 WITNESS PROTECTION HEALTH RECORDS

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

8.15 CONTROLLED DRUGS REGIME

NHS England in conjunction with the NHS Business Services Authority has established procedures for handling information relating to controlled drugs. This guidance includes conditions for storage, retention and destruction of information. Where information about controlled drugs is held please refer to NHS England guidance[8].

8.16 ASYLUM SEEKER RECORDS

Any service provided to any client must have a record. For reasons of clinical continuity or professional conduct, records for asylum seekers must be treated in exactly the same way as other health records. Where the asylum seeker is given a patient held record, the provider must satisfy themselves that they have a record of what they have done in case of litigation or matters of professional conduct.

8.17 OCCUPATIONAL HEALTH RECORDS

Occupational health records are not part of the main staff record and for reasons of confidentiality they are held separately. However, it is permitted for reports or summaries to be held in the main staff record where these have been requested by the employer and agreed by the staff member. When occupational health records are outsourced, the organisation must ensure that any contractor can retain the records for the necessary period after the termination of service for purposes of adequately recording any work based health issues.

8.18 RECORDS OF NON-NHS FUNDED PATIENTS TREATED ON NHS PREMISES

Where records of individuals who are not NHS or social care funded are held in the record keeping systems of NHS or social care organisations, they must be kept for the same minimum retention periods as other records outlined in this Code. The same levels of security and confidentiality will also apply.

8.19 PATIENT/CLIENT HELD RECORDS

Where it is necessary to leave records with the individual who is the subject of care, it must be indicated on the records that they remain the property of the issuing

[8] http://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf

organisation and include a return address if they are lost. The Trust must be able to produce a record of their work which includes services delivered in the home where the individual holds the record. Upon the termination of treatment where the records are the sole evidence of the course of treatment or care, they must be recovered and given back to the issuing organisation and the service needs to have a tracking process in place that clearly documents when records have been given back.
A copy can be provided if the individual wishes to retain a copy of the records. Where the individual retains the actual record after care, the organisation must be satisfied it has a record of the contents. An example is a child's red book where the parent retains the record but the contents are also recorded in the health visiting file.

8.20 RECORDS DEALT WITH UNDER THE NHS TRUSTS AND PRIMARY CARE TRUSTS (SEXUALLY TRANSMITTED DISEASE) DIRECTIONS 2000

The directions impose an additional obligation of confidentiality on employees and trustees of NHS Trusts, Clinical Commissioning Groups, local authority public health functions and those providing services under contract regarding information about sexually transmitted diseases.
This obligation differs from patient confidentiality generally as it prohibits some types of sharing, but enables sharing where this supports treatment of patients. For this reason it is common for services dealing with sexually transmitted diseases to partition their record keeping systems to comply with the directions and more generally to meet patient expectations that such records should be treated as particularly sensitive.

9. EQUALITY IMPACT ANALYSIS

As part of its development, this document was analysed to consider / challenge and address any detrimental impact the policy may have on individuals and or groups protected by the Equality Act 2010. This analysis has been undertaken and recorded using the Trust's analysis tool, and appropriate measures will be taken to remove barriers and advance equality of opportunity in the delivery of this policy / procedure

10. FREEDOM OF INFORMATION EXEMPTION ASSESSMENT

Under the Freedom of Information Act (2000) we are obliged to publish our policies on the Trust's website, unless an exemption from disclosure applies. As part of its development, this policy was assessed to establish if it was suitable for publication under this legislation. The assessment aims to establish if disclosure of the policy could cause prejudice or harm to the Trust, or its staff, patients, or partners. This assessment has been undertaken using the Trust's Freedom of Information Exemption Guide, and will be reviewed upon each policy review.

11. INFORMATION GOVERNANCE ASSESSMENT

This Policy has been analysed to ensure it is compliant with relevant information law and standards as in place at the time of approval, and are consistent with the Trust's interpretation and implementation of information governance components such as data protection, confidentiality, consent, information risk, and records management. Compliance will be reviewed against any changes to legislation / standards or at the next review of this document.

12. SAFEGUARDING

All staff have a responsibility to promote the welfare of any child, young person or vulnerable adult they come into come into contact with and in cases where there are safeguarding concerns, to act upon them and protect the individual from harm.
All staff should refer any safeguarding issues to their manager and escalate accordingly in line with the Trust Safeguarding Families Policy and Local Safeguarding Children/Adult Board processes.

13. MONITORING

The effective application of this policy, including adherence to any standards identified within will be subject to monitoring using an appropriate methodology and design, such as clinical audit.
Monitoring will take place on a biannual basis and will be reportable to the Quality Group via the Clinical Effectiveness and Quality Improvement Team.

14. REVIEW

This policy will be reviewed three-yearly unless there is a need to do so prior to this; e.g. change in national guidance.

15. REFERENCES

Data Protection Act 2018
Equality Act 2010
Freedom of Information Act 2000
Gender Recognition Act 2004
General Data Protection Regulation 2018